The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STATE OF WASHINGTON, et al.

Plaintiffs,

v.

UNITED STATES DEPARTMENT OF STATE, et al.,

Defendants.

No. 2:18-cv-01115-RSL

PRIVATE DEFENDANTS' REPLY IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT

Table of Contents

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

Argument

Suppose that in the wake of *Brown v. Board of Education*, 347 U.S. 483 (1954), and *Bolling v. Sharpe*, 347 U.S. 497 (1954), federal agencies stopped segregating school services *but* failed to satisfy all APA technicalities in doing so. Could recalcitrant states use an APA suit to force federal officials *to reinstitute segregation policies*? Of course not. The Constitution is always paramount.

Suppose that in the wake of *United States v. Windsor*, 570 U.S. 744 (2013), and *Obergefell v. Hodges*, 135 S. Ct. 2584 (2015), federal tax agencies ceased discriminating against same-sex couples *but* violated an APA technicality in doing so. Could states use the APA to force federal officials *to reinstitute the discriminatory policies*? No. The Constitution still prevails.

And yet here we are. In the wake of *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2226 (2015) ("Content-based laws . . . are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests."), *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) ("[T]he creation and dissemination of information are speech within the meaning of the First Amendment."), *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 253 (2002) ("The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it."), and *Bartnicki v. Vopper*, 532 U.S. 514, 529-30 (2001) ("[I]t would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party.")—not to mention *District of Columbia v. Heller*, 554 U.S. 570 (2008)—the State Department rightly ceased violating Defense Distributed and the Second Amendment Foundation's constitutional rights by freeing them from ITAR's content-based prior restraint. But now recalcitrant states want an order forcing federal officials to re-impose that unconstitutional regime on the theory that the "*First Amendment is irrelevant*." Dkt. 186 at 20. That cannot be so. *See Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

On the merits, the Plaintiff States' attempt to have the Administrative Procedure Act override the First Amendment can never work. For in this Union, states can neither violate the Constitution themselves nor commandeer the federal government to do their unconstitutional bidding. But the merits should not be reached because of a more fundamental fault: no standing.

The Plaintiff States have suffered no legally cognizable injury at all, let alone one inflicted by a defendant in this case. Nor do traceability or redressability exist because the whole world already has the files at issue, and always will. Defense Distributed published them to the internet's public domain for **five full days** before the preliminary injunction, and ever since then, a multitude of independent users has persistently and increasingly republished them *despite the injunction*. This state of affairs simply cannot be controlled by a court judgment. The case must be dismissed.

I. Standing does not exist.

The Court lacks subject-matter jurisdiction for five separate reasons, the most drastic of which is lack of standing. Dkt. 174 at 4-8. These issues must be evaluated in full—not discounted due to prior briefing—because "federal courts have a continuing, independent obligation to determine whether subject matter jurisdiction exists." *Mashiri v. Dep't of Educ.*, 724 F.3d 1028, 1031 (9th Cir. 2013). That obligation is especially strong because of an important new decision about the legal doctrine being invoked and because of new jurisdictional evidence.

The Plaintiff States give standing short shrift. In a quiet footnote, their most recent filing says nothing but that "previous briefing . . . addresses the Private Defendants' already-rejected challenges to standing." Dkt. 186 at 9 n.9. This will not suffice. Fortunately, though, the Plaintiff States supplied their true view about standing law in another brief. It just so happens to have been submitted to another court.

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

A. The Plaintiffs States' own filings defeat their standing argument.

Standing questions just like the ones in this case arose in *United States v. Texas*, 136 S. Ct. 2271 (2016) (per curiam) (No. 15-674). There, fifteen of the instant Plaintiff States filed an *amicus* brief focusing on standing law for state APA actions against the federal government. Amicus Brief of the States of Washington, et al. in Support of Petitioners, *United States v. Texas*, 136 S. Ct. 2271 (2016) (per curiam), 2016 WL 922867. That brief's reasoning shows why no standing exists here.

First, the Plaintiff States' Supreme Court brief said that state standing did not exist because that case's plaintiffs "filed this suit, not because they are suffering any meaningful harm, but rather to achieve a political goal that they could not achieve through the political process." *Id.* at *1. So too here. The plaintiffs' politicians loathe citizens who speak about realizing the Second Amendment's guarantees; but the speech they want to ban has broken no law, state or federal.

Next, the Plaintiff States' Supreme Court brief said that state standing did not exist because that state's injury argument "relies on a false premise - that the [agency action] requires States to do anything at all." *Id.* at *3. So too here. The Temporary Modification and License require literally nothing of the Plaintiff States, who remain as free as they have ever been to both enact and enforce criminal laws of their choosing (subject, of course, to the Constitution).

Next, the Plaintiff States' Supreme Court brief said that "self-inflicted 'harms'" cannot suffice to create a state's standing. *Id.* at 5. So too here. If the Plaintiff States decide to update security practices because of technological change, "doing so will be a state choice, 'not the result of federal coercion.'" *Id.* at *4 (quoting *Texas v. United States*, 106 F.3d 661, 666 (5th Cir. 1997)).

If the rules that the Plaintiff States embraced in their Supreme Court brief were applied here, they would compel the conclusion that no standing exists. The Plaintiff States should be held to their own standards, even when political tables have turned.

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

B. Traceability and redressability are missing.

This action's lack of traceability and redressability gets worse with every passing day. In March, the Private Defendants supplied a wealth of evidence proving that the "computer files that the Plaintiff States have made this litigation about already belong to the public domain." Dkt. 174 at 3 & nn.5-6. Since then, even more authority confirms the standing problem's factual basis.

Just last month, a leading technologist confirmed that the internet's publication of Defense Distributed's digital firearms information is "unstoppable": "There is no way to stop the anonymous file sharing of 3D-printed guns online." Jake Hanrahan, *3D-printed guns are back, and this time they are unstoppable,* Wired Magazine, May 20, 2019, available at http://bit.ly/2MtWcZf. "As of now," the report says, the "thousands many more 3D-printed gun enthusiasts connected to each other worldwide" have "essentially let the cat out the bag." *Id.* Defense Distributed's files are "available for free." *Id.* It is "already too late to stop." *Id.*

This reality's technical basis bears emphasis. "A decentralised network of gun-printing advocates is mobilising online, they're anonymously sharing blueprints, advice and building a community." *Id.* "Unlike previous attempts to popularise 3D-printed guns, this operation is entirely decentralised." *Id.* "There's no headquarters, no trademarks, and no real leader." *Id.* Hosts include a network of gun-printing advocates that communicate across multiple peer-to-peer ("P2P") networks beyond any government's reach. *See* John Crump, *The Unstoppable 3D Gun Revolution Continues to Heat Up*, Ammoland, May 30, 3019, available at http://bit.ly/2WkgpjV. "Since there is not a central server, there is nothing to shut down." *Id.* "If one node is shut down multiple other nodes pop up." *Id.* The "distributors of these files seem to be unstoppable." *Id.*

Hence, all of the files at issue in this case remain easily accessible by way of rudimentary Google queries. Every website exhibited in the Private Defendants' last brief remains intact,

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

continuing to make their files available for anyone to download for free. *See* Dkt. 174 at 3 nn.5-6.[1]

Critically, all of this has taken place despite the Court's entry of a preliminary injunction that does everything the Plaintiff States seek in their prayer for permanent relief. In effect, the preliminary injunction has proven to be impotent. This experience shows that the requested final judgment will be ineffective at redressing the Plaintiff States' supposed injuries.

C. *Parens patriae* standing cannot be used against the federal government.

The Plaintiff States' only serious standing argument invokes the *parens patriae* doctrine, which sometimes "allows a State to sue in a representative capacity to vindicate its citizens' interests." *Gov't of Manitoba v. Bernhardt*, 923 F.3d 173, 178 (D.C. Cir. 2019). But as a matter of law, the Plaintiff States cannot use *parens patriae* here because their claims are against the federal government. "The traditional rule, the so-called '*Mellon* bar,' declares that a State lacks standing as *parens patriae* to bring an action against the federal government." *Id.* at 179.

The solution suggested by previous briefs was *Massachusetts v. EPA*, 549 U.S. 497 (2007). According to the Plaintiff States' prior filings, footnote 17 of *Massachusetts v. EPA* eliminated this limitation and held that states *can* use *parens patriae* standing against the federal government. Dkt. 68 at 11. But a new precedent decisively establishes that the Plaintiff States' reading of *Massachusetts v. EPA* is wrong. Footnote 17 does not change standing law as they say. The bar on states using *parens patriae* standing against the federal government remains.

Last month, the D.C. Circuit confronted and rejected the exact *parens patriae* argument being made by the Plaintiff States here. *Bernhardt*, 923 F.3d at 181-83. There, as here, a state tried to argue that footnote 17 of *Massachusetts v. EPA* lets states employ *parens patriae* standing in APA actions against the federal government. *Id.* But in a unanimous and thorough decision,

[1] Meanwhile, the summary judgment record indicates that Defense Distributed and the Second Amendment Foundation are the only Second Amendment advocates to have received any serious legal attention from the Plaintiff States.

the D.C. Circuit rejected that argument: "In the end, we are unpersuaded by Missouri's argument that *Massachusetts v. EPA* alters our longstanding precedent that a State in general lacks *parens patriae* standing to sue the federal government." *Id.* at 183.

The argument stemming from footnote 17 is both an incorrect reading of *Massachusetts v. EPA* and wrong in principle. "The general supremacy of federal law" means "that the federal *parens patriae* power should not, as a rule, be subject to the intervention of states seeking to represent the same interest of the same citizens." *Id.* For that reason, a "state can not have a quasi-sovereign interest because" matters of federal law "fall[ ] within the sovereignty of the Federal Government." *Id.* (omission in original).

Bernhardt is decisive. *Massachusetts v. EPA* did not eliminate the bar on states using *parens patriae* standing against the federal government. The Plaintiff States have no answer to this categorial flaw in their case, which is why their latest brief ignores the issue entirely.

II. Defense Distributed should be dismissed for lack of personal jurisdiction.

A. No waiver occurred.

The Plaintiff States argue that Defense Distributed waived its personal jurisdiction defense because Rule 12(h)(1)(A) supposedly says that "a party waives the defense of lack of personal jurisdiction by 'omitting it from a motion' under Rule 12." Dkt. 186 at 19. But the cited provision never says that (and neither does sole cited case). The waiver argument plainly misreads the rule.

What Rule 12(h)(1)(A) *does* say is that waiver occurs if the defense is omitted a "from a motion *in the circumstances described in Rule 12(g)(2)*." Fed. R. Civ. P. 12(h)(1)(A) (emphasis added). The "circumstances described in Rule 12(g)(2)," in turn, exist by definition only when a defendant files *multiple Rule 12 motions*:

> Except as provided in Rule 12(h)(2) or (3), a party that makes a motion under this rule must not make ***another motion under this rule*** raising a defense or objection that was available to the party but omitted from its earlier motion.

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

Fed. R. Civ. P. 12(g)(2) (emphasis added).[2] Not so here.

Defense Distributed made only one motion under Rule 12. Dkt. 114. They never filed "another motion under this rule" (Rule 12) because the instant summary-judgment filings are under Rule 56. These are not "the circumstances described in Rule 12(g)(2)." No Rule 12(h)(1)(A) waiver occurred.

Support for Defense Distributed's method of challenging personal jurisdiction comes from Rule 12(b)'s use of "must" and "may." That provision says that litigants "must" assert a personal jurisdiction defense in a pleading (Defense Distributed did that, *see* Dkt. 81 at 42), and that litigants "may" assert the defense in a Rule 12 motion. Fed. R. Civ. P. 12(b). Since "may" is permissive, asserting the defense in a Rule 12 motion is not required. It is optional.

Support for Defense Distributed's method of challenging personal jurisdiction also comes from Rule 12(h)(1)(B)(ii)'s use of "either" and "or." That provision shows that the defense of personal jurisdiction is preserved where, as here, the defendant has "either" made it by a Rule 12 motion "or" "include[d] it in a responsive pleading." Fed. R. Civ. P. 12(h)(1)(B)(ii).

This is not a "convoluted non-waiver theory." Dkt. 186 at 19. It is straightforward construction that gives a logical meaning to each part of Rule 12. The Plaintiff States' position, in contrast, would work only if Rule 12(b) changed "may" to "must" and Rule 12(h)(1)(B)(ii) changed "either" and "or" to "both" and "and." As it stands, Rule 12 says no such thing.

B. DEFCAD's free downloads do not create minimum contacts.

Substantively, the Plaintiff States say that personal jurisdiction exists because Defense Distributed's website (DEFCAD) "actively invites visitors to download CAD files." Dkt. 186 at 19. But the Plaintiff States did not plead anything about how interactive the website is, let alone

[2] Those circumstances existed in the lone cited case because the defendant filed *multiple* Rule 12 motions. *Schnabel v. Lui*, 302 F.3d 1023, 1027-28 (9th Cir. 2002).

prove it with any evidence. The complaint says nothing more than that the website makes files "available for download," Dkt. 29 at 4, 10, because that is the fact of the matter.

Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997), does not support personal jurisdiction here. The Plaintiff States try to shoehorn Defense Distributed's situation into this quotation: "If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper." Dkt. 186 at 19 (quoting *Zippo*, 952 F. Supp. at 1124). But the keystone fact of business "contracts with residents" is missing. The complaint never speaks of the website creating contractual relationships for these downloads, and neither does evidence. *See* Dkt. 174-01 at 3 ("Defense Distributed posted . . . on DEFCAD for free download by the public.").

The Court should look not to the sentence quoted by the Plaintiff States, but to the one right after it. DEFCAD fits squarely within what *Zippo* frames as the "opposite end" of the spectrum. *Zippo*, 952 F. Supp. at 1124. Under *Zippo*, Defense Distributed's online file publications constitute the kind of "passive" website activity that does *not* confer personal jurisdiction:

> At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. *At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction.*

Id. at 1124 (emphasis added) (citations omitted).

Besides quoting the wrong part of *Zippo*, the Plaintiff States refuse to address three critical jurisdictional faults in their position. They never address the rule that "contacts count towards purposeful availment only if they are created by the 'defendant himself'—not if they are created by 'plaintiffs or third parties.'" Dkt. 174 at 10 (quoting *Walden v. Fiore*, 571 U.S. 277, 284

(2014)). They never address the rule that "'minimum contacts' analysis looks to the defendant's contacts with *the forum State itself*, not the defendant's contacts with *persons who reside there*." *Id.* (quoting *Walden*, 571 U.S. at 285). And they never address the rule that hypothesized future forum contacts cannot count towards what must be a present purposeful availment inquiry. *Id.* at 10-11. Each of these unanswered arguments presents an independent reason to dismiss the case against Defense Distributed for lack of personal jurisdiction.

III. The APA cannot require abridgement of First Amendment freedoms.

Two crucial sets of authority about the Constitution's interaction with the APA have gone totally ignored. First is 5 U.S.C. § 702, which says that, even when the APA's internal thresholds for relief are met, reviewing courts must still determine whether or not there is a "duty of the court to . . . deny relief on any other appropriate legal or equitable ground." 5 U.S.C. § 702. Thus, to the extent that an APA plaintiff's requested relief would violate the First Amendment, § 702 requires the reviewing court to "deny relief" on this Constitutional "ground." *See* Dkt. 174 at 20.

Indeed, this would be required even in § 702's absence due to elementary principles of constitutional law. *See infra* at 1. Like every other statute, the APA is subject to the rule that "Congress shall make no law . . . abridging the freedom of speech." U.S. Const. Am 1. So even if the APA purported to authorize judgments that abridge the freedom of speech (it does not), the First Amendment's overriding command would nullify it.

The other ignored authorities are *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958), *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960), and *Perry v. Schwarzenegger*, 591 F.3d 1147, 1160-61 (9th Cir. 2010). They stand for the proposition that courts cannot issue orders of any kind—even things as relatively commonplace as discovery orders—that have the "practical effect" of denying First Amendment rights. Dkt. 174 at 20. This doctrine is one of the "appropriate

legal or equitable ground[s]" that has to be evaluated before APA relief can be issued.

All of these principles carry special weight where, as here, the law's constitutional infirmity comes not just from instances of its enforcement against the citizenry, but also from the chilling effect created by its mere existence on the books. *See Laird v. Tatum*, 408 U.S. 1, 11 (1972) ("constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights."); *Dana's R.R. Supply v. Att'y Gen., Flo.*, 807 F.3d 1235, 1241 (11th Cir. 2015) ("Litigants who are being 'chilled from engaging in constitutional activity,' . . . suffer a discrete harm independent of enforcement . . . .").

None of this is addressed in the Plaintiff States' brief. Talk about what a court can and cannot consider under *Chenery* is inapposite, for that goes only to the predicate determination of what the APA's internal procedural requirements entail. *After* the internal APA analysis occurs, courts are always obliged to ensure that a sought-after judgment does not violate the Constitution.

IV. The Plaintiff States' APA claims against the Federal Defendants fail.

A. Notification issues do not support any relief.

The Plaintiff States continue to argue that "[t]he Temporary Modification and Letter deregulating 3D-printed firearm files violate AECA's congressional notice provisions . . . ." Dkt. 186 at 1. But they never show why notification requirements at 22 U.S.C. § 2778(f) apply to the License or Temporary Modification. In truth, "[n]othing has been removed from the USML by the Settlement Agreement, and, thus, no section 38(f) notice was required as a result of the Settlement Agreement." Dkt. 48-1 at 110.

Additionally, the Plaintiff States fail to realize that, apart from a notification about a commodity or item itself, no *separate* notification for technical data about a commodity or item is needed. "The jurisdiction of the technical data follows the jurisdiction of the related commodity

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

or item." 78 Fed. Reg. 22740, 22748 (April 16, 2013). This follow-on structure is how all transfers to the EAR under export control reform work. *See* 81 Fed. Reg. 70340 (Oct. 12, 2016) at 70357; 81 Fed. Reg. 49531 (July 28, 2016) at 49538 and 49539; 79 Fed. Reg. 37536 (July 1, 2014) at 37545; 79 Fed. Reg. 27180 (May 13, 2014) at 27185 to 27186 and 27188; 79 Fed. Reg. 34 (Jan. 2, 2014) at 41, 44, 45, and 46; 78 Fed. Reg. 40922 (July 8, 2013) at 40928, 40929, and 40931; 78 Fed. Reg. 22740 (April 16, 2013) at 22757 and 22758.

Even if the License and Temporary Modification constitute removals (they do not), notification of the proposed removal of firearms and associated technical data (which includes the subject files) was reportedly provided to Congress on February 4, 2019. Dkt. 174 at 18. Since this notice, Congress could have blocked the removal (by, for example, Joint Resolution), but has chosen *not* to do so.

B. There was no reversal of longstanding regulation with regard to the license or temporary modification.

The Plaintiff States are wrong to assert that the State Department's actions entail an "abrupt reversal of its longstanding regulation of the subject files." Dkt. 186 at 1. The State Department has disclaimed control of public speech under the ITAR for 30 years.

In 1980, responding to concerns that a vague footnote in the ITAR could be read to restrain public speech, the State Department announced: "[a]pproval is not required for publication of data within the United States . . . [the footnote] does not establish a prepublication review requirement." Dkt. 158-3 at DOSWASHINGTONSUP00342-43. The State Department then removed the footnote from the ITAR, expressly stating its intent to address First Amendment concerns. *See* 49 Fed. Reg. 47,682, 47,683 (Dec. 6, 1984).

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

In addition to the State Department's express removal of any prior restraint in 1984, the ITAR expressly excludes from its scope information found in the public domain. *See* 22 C.F.R. § 120.10(b). Any reasonable person reading ITAR's expansive definition of "public domain" at 22 C.F.R. § 120.11 would conclude that U.S. persons without connections to foreign enterprises can publish technical information in public venues without U.S. government preapproval. *See, e.g.*, *United States v. Edler Indus.*, 579 F.2d 516, 521 (9th Cir. 1978) ("So confined, the statute and regulations are not overbroad [or] an unconstitutional prior restraint on speech.").

In the *Bernstein* litigation[3], the State Department again confirmed that the ITAR does not impose a prior restraint on public speech, noting: "Since 1984, the ITAR has been amended in order to indicate more clearly that publicly available information and academic exchanges are not treated as technical data." Ex. S at 10, ¶ 20 (Second Declaration of William J. Lowell, Department of State Office of Defense Trade Controls, *Bernstein v. U.S. Dep't of State*, No. C 95-0582 (N.D. Cal.) (July 26, 1996)). It declared: "the Department does not seek to regulate the means themselves by which information is placed in the public domain." *Id.* at 11, ¶ 22 (emphasis in the original). Moreover, it forcefully rejected any interpretation of ITAR's public domain provision as imposing a prior restraint on public speech as "by far the most **un**-reasonable interpretation of the provision." *Id.* at 23 (Defendants' Opposition to Plaintiff's Motion for Summary Judgment and in Further Support of Defendants' Motion for Summary Judgment, *Bernstein v. U.S. Dep't of State*, No. C 95-0582 (N.D. Cal.) (Aug. 30, 1996)) (emphasis in original).

[3] *See, e.g.*, *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132 (9th Cir.), reh'g in banc granted, 192 F.3d 1308 (9th Cir. 1999); *Bernstein v. U.S. Dep't of State*, 974 F. Supp. 1288 (N.D. Cal. 1997); *Bernstein v. U.S. Dep't of State*, 945 F. Supp. 1279 (N.D. Cal. 1996); *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426 (N.D. Cal. 1996)

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

The 2013 State Department letter to Defense Distributed demanding the takedown of the subject files was the abrupt reversal of longstanding regulation. The State Department then issued a proposed rule to restrain public speech. *See* 80 Fed. Reg. 31,525, 31,528 (June 3, 2015). This proposal drew over 9,000 public comments.[4] Most commenters opposed the proposal, including technology industry leaders (e.g., IBM, GE, and others), export control attorneys, and even former State Department employees. *See, e.g.*, Dkt. 63-1 at 38 ("The ITAR proposed requirement for USG authorization to put information into the 'public domain' in 120.11(b) is a reversal of actions 30 years ago to comply with the free speech first amendment to the Constitution."). Not surprisingly, the ITAR was never amended to impose a prior restraint.

C. The record shows compelling justifications for the Temporary Modification and License.

Consistent with the 30-year history of the State Department disclaiming any control of public speech under the ITAR, the record includes decades of Justice Department legal opinions concluding that controlling public speech under the ITAR violates the First Amendment.[5] These opinions pose a compelling justification—"the licensing requirement is presumptively unconstitutional as a prior restraint on speech protected by the First Amendment."[6]

The Plaintiff States further argue that the Justice Department opinions are irrelevant because "the Federal Defendants have not purported to rely on any of these statements . . . ." Dkt. 186 at 24. But there can be no reasonable dispute that the State Department relied on the Justice Department statements because those opinions are part of the Administrative Record and the State

[4] *See* Ex. T (Regulations.gov, "International Traffic in Arms: Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions," *available at* http://bit.ly/2XtSDn0 (last visited June 6, 2018)).
[5] *See* Dkt. 48-1 at Exhibits A-D; Dkt. 158-3 at DOSWASHINGTONSUP00236-252, 239 at n.7, 254-266, 268-272, 274-288, 290-333, and 313; Dkt. 174 at 14-16.
[6] *See* Dkt. 48-1 at 20.

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

Department *publicly stated* that it settled the case based on the Justice Department's advice that the agency would lose on First Amendment grounds. Dkt. 35-1 at 5.

D. The proposed transfer is valid.

As detailed in Private Defendants' Motion for Summary Judgment, the proposed rule offers various justifications for the list transfers, including reduced burden hours, reduced costs, and decreased taxpayer costs. Dkt. 174 at 17-18. Plaintiffs do not provide any reasonable explanation for why these justifications do not satisfy the APA. Instead, the Plaintiff States harp on "106,000 emails from members of the public between July 23 and July 27, 2018, urging the Department not to exempt 3D-printable guns." Dkt. 186 at 3. But according to the record, these emails came not from actual individuals, but from a BOT conducting a targeted spam campaign on behalf of an interest group. *See* Dkt. 184-11 at WASHAR0003428; *id.* at WASHAR0003435 ("These are not individuals attempting to contact the Secretary, but this appears to be a BOT conducting a targeted spam campaign . . . ."); *see also* Dkt. 184-5 at WASHAR0000008-9.

The Plaintiff States further argue that the State Department's action was arbitrary and capricious because of "multiple letters from Congressional leaders urging reconsideration of the deregulation of 3D-printable gun files; detailed comment letters from U.S. Senators and public policy organizations," Dkt. 186 at 3; and because the State Department allegedly failed to address Democrat staffer requests. Dkt. 186 at 3-5. But Democrat concerns were countered by requests from over 100 Republican members of Congress. *See, e.g.*, Dkt. 184-6 at WASHAR0001093; Dkt. 184-6 at WASHAR0001098; Dkt. 184-6 at WASHAR0001091-1092; Dkt. 184-8 at WASHAR0002058-2068; Dkt. 184-10 at WASHAR0003034-3035.

No merit lies in the Plaintiff States' complaints about comments not receiving bespoke responses. Several well-established rules of administrative procedure make this clear.

A failure to respond to comments means nothing unless it somehow "demonstrates that the agency's decision was not 'based on a consideration of the relevant factors.'" *Thompson v. Clark*, 741 F.2d 401, 409 (D.C. Cir. 1984). None of the Plaintiff States' cherrypicked comments do so.

Comments without "meaningful analysis or data" certainly warrant no response, and neither do comments that "brought to the attention of the agency nothing which it had not already considered." *Id.* These rules apply to virtually all of the Plaintiff States highlighted comments, which add nothing meaningful or new to the State Department's deliberative calculus.

This was also an instance in which agencies need not respond to comments that are "diametrically" or "directly opposed" to the policy's overall "thrust." *Sherley v. Sebelius*, 689 F.3d 776, 784-85 (D.C. Cir. 2012). In other words, the State Department had no obligation to "comment on policy-based challenges to the basic premise of the proposed rule where the agency has already chosen a particular reconciliation of conflicting congressional directives and has previously explained its reasoning." *Baltimore Gas & Elec. Co. v. United States*, 817 F.2d 108, 116 (D.C. Cir. 1987).

Under these principles, the Federal Defendants need not have responded to the Plaintiff States' favorite comments with anything more than the existing explanations. The Plaintiff States' side of this political debate did not get mistreated. They were heard fairly. They just lost.

Conclusion

The Court should issue a summary judgment dismissing this action for lack of subject-matter jurisdiction. Alternatively, the Court should issue a summary judgment dismissing the Private Defendants from the action. In the further alternative, the Court should issue a summary judgment that the Plaintiff States take nothing. Any relief that is awarded to the Plaintiff States should be restricted to conduct taking place in the Plaintiff States' jurisdictions.

Beck Redden LLP
1221 McKinney Street, Suite 4500
Houston, Texas 77010
(713) 951-3700

Date: June 7, 2019.

Respectfully submitted,

BECK REDDEN LLP

/s/Charles Flores
Charles Flores
cflores@beckredden.com
Beck Redden LLP
1221 McKinney, Suite 4500
Houston, TX 77010
Phone: (713) 951-3700
*Admitted Pro Hac Vice

Attorney for Defendant
Defense Distributed

FARHANG & MEDCOFF

/s/Matthew Goldstein
Matthew Goldstein
Farhang & Medcoff
4801 E. Broadway Blvd., Suite 311
Tucson, AZ 85711
Phone: (202) 550-0040
mgoldstein@farhangmedcoff.com
*Admitted Pro Hac Vice

ARD LAW GROUP PLLC
/s/Joel B. Ard
Joel B. Ard, WSBA # 40104
joel@ard.law
Ard Law Group PLLC
P.O. Box 11633
Bainbridge Island, WA 98110
Phone: (206) 701-9243

Attorneys for Defendants
Defense Distributed, Second Amendment
Foundation, Inc., and Conn Williamson

CERTIFICATE OF SERVICE

I certify that on June 7, 2019, I used the CM/ECF system to file this document with the Clerk of the Court and serve it upon all counsel of record.

/s/Charles Flores
Charles Flores
cflores@beckredden.com
Beck Redden LLP
1221 McKinney, Suite 4500
Houston, TX 77010
Phone: (713) 951-3700
*Admitted Pro Hac Vice

Attorney for Defendant
Defense Distributed

EXHIBIT S

ORIGINAL

FRANK W. HUNGER
Assistant Attorney General
MICHAEL J. YAMAGUCHI
United States Attorney
MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198
VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460
Attorneys for the Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN Plaintiff, v. UNITED STATES DEPARTMENT OF STATE et al., Defendants.	C 95-0582 MHP **SECOND DECLARATION OF WILLIAM J. LOWELL DEPARTMENT OF STATE OFFICE OF DEFENSE TRADE CONTROLS**

I, William J. Lowell, do hereby state and declare as follows:

1. I am the Director of the Office of Defense Trade Controls ("ODTC"), Bureau of Political-Military Affairs, United States Department of State. I have held this position since November 27, 1994. I am the same William J. Lowell who submitted a declaration to this Court filed on August 5, 1995, in connection with defendants' motion to dismiss. I submit this declaration in support of defendants' motion for summary judgment. This declaration will describe the State Department's actions in connection with the

commodity jurisdiction requests of Daniel J. Bernstein at issue in this case. In addition, I will discuss some of the regulatory provisions that are at issue in this case. The statements made herein are based on my personal knowledge and information obtained in the course of my official duties.

I. Statute and Regulations[1]

2. The Department of State administers the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Subchapter M, Parts 120 to 130, under the authority contained in Section 38 of the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778. Under the AECA, the President is authorized to regulate the export and import of defense articles and services "in furtherance of world peace and the foreign policy and national security of the United States." 22 U.S.C. § 2778(a)(1). The President delegated this authority to the Secretary of State, pursuant to which the Department regulates the export of defense articles designated on the United States Munitions List ("USML"), 22 C.F.R. Part 121, and related technical data and defense services.

3. The category of the USML relevant to this case is Category XIII(b)(1), which lists as defense articles "[c]ryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems" -- except cryptographic equipment and software as excluded

[1] Parts I and II of this declaration are generally derived from my first declaration, and are re-stated or summarized for the convenience of the Court.

from Category XIII(b)(1) as described in the regulations. 22 C.F.R. § 121.1 XIII(b)(1).

4. As stated in my first declaration, cryptographic devices and software are included on the United States Munitions List in order to assure that such items do not fall into dangerous hands abroad, or otherwise be deployed against the interests of the United States and its allies. Throughout history, governments of all nations have relied on intelligence information to cope with wars and other international crises. For example, the ability of the United States and its allies in World War II to break German "ENIGMA" and Japanese "PURPLE" coded communications of the axis forces was critical in shortening the war and saving lives. When U.S. armed forces are deployed, gathering intelligence information on the activities of hostile forces is critical to ensuring the effective accomplishment of their mission with minimal loss of life. Cryptographic devices and software can be applied in a military setting against U.S. forces, or against U.S. intelligence gathering efforts. The United States seeks to control the export of certain cryptographic products and software in order to protect the United States' ability to gather foreign intelligence on military, national security, and foreign policy matters. See Declaration of William P. Crowell, Deputy Director of the National Security Agency.

5. As discussed below, however, the State Department does not apply the ITAR's export controls on cryptographic software and technical data to limit the ability of individuals who merely seek to publish scientific ideas or exchange information in an academic setting in the United States. In addition, the Department does not control every kind of cryptographic product and software as defense

articles on the USML. Some cryptographic products and software are not subject to USML controls, and others that could be covered by the USML can instead be transferred to the export jurisdiction of the Commerce Department. In addition, cryptographic products and software that remain covered by the USML are not "banned" from export, but are controlled through the licensing process.[2] In fact, many items on the USML are approved for exportation to countries around the world. The licensing decision takes into account a combination of factors, including the sensitivity of the technology, the identity of the end-user, the declared end-use of the commodity, and foreign policy and national security interests.

II. State Department Review of Bernstein CJ Requests

A. June 1992 First Bernstein CJ Request

6. The ITAR contains a procedure -- the commodity jurisdiction procedure -- to be used when doubt exists as to whether a particular article or service is included on the USML. 22 C.F.R. § 120.4. This procedure is not a mandatory requirement. Rather, upon written request, the Office of Defense Trade Controls of the State Department will provide such a determination. 22 C.F.R. § 120.4(a). A person may appeal such a determination to the Deputy Assistant Secretary of State for Export Controls, and then to the Assistant Secretary of State for Political-Military Affairs. See Tab 2 (DTC publications describing the CJ process).

---

[2] Certain prohibitions on export do exist, mainly with respect to states which the Secretary of State has determined are sponsors of international terrorism -- Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

7. By letter dated June 30, 1992, Dr. Bernstein submitted to the State Department a commodity jurisdiction request for Snuffle 5.0 software. Tab 3.

8. By letter dated August 20, 1992, the Office of Defense Trade Controls responded to Dr. Bernstein's commodity jurisdiction request for Snuffle 5.0 software. Tab 4. The Department advised Dr. Bernstein that the commodity referenced in his request (Snuffle 5.0) is designated as a defense article under Category XIII(b)(1) of the United States Munitions List and is subject to the licensing jurisdiction of the State Department. Dr. Bernstein was advised that a license from the State Department was required prior to the exportation of this commodity.[3]

---

[3] A substantial amount of correspondence is also included in the record of Dr. Bernstein's CJ determination, and is submitted again herewith for completeness and the convenience of the Court. **Tabs 5 and 6**: Dr. Bernstein sent two letters dated March 19, 1993 and April 2, 1993, to the Office of Defense Trade Controls asking various questions concerning the ITAR. **Tab 7:** By letter dated May 20, 1993, Dr. Bernstein also wrote to Congressman Dellums on this matter. **Tab 8:** By letter dated May 24, 1993, Congressman Dellums inquired of the State Department concerning Dr. Bernstein's letters. **Tabs 9 and 10:** By letters dated May 25 and 27, 1993, the Department responded to Dr. Bernstein's correspondence. **Tab 11:** By letter dated June 22, 1993, the Department responded to Congressman Dellums' inquiry. **Tabs 12 and 13:** By letter dated June 30, 1993, Dr. Bernstein again corresponded with the State Department, and the Department responded by letter dated (circa) July 7, 1993. **Tab 14:** By letter dated September 20, 1993, Dr. Bernstein responded to the Department's July 7 letter. **Tab 15:** By letter dated July 19, 1993, the Department responded to Dr. Bernstein's request for a copy of newly published ITAR amendments. **Tab 19**: By letter dated October 5, 1993, the Department provided Mr. Bernstein with a booklet on ITAR registration procedures.

C. July 1993 Second Bernstein CJ Request

9. By letter dated July 15, 1993, Dr. Bernstein submitted a second commodity jurisdiction request, which he designated DJBCJF-2 through 6. Tab 16.

10. By letter dated July 26, 1993, the Department advised Dr. Bernstein that his submission had been consolidated and referred to the Departments of Commerce and Defense for their recommendations. Tab 17.

11. In response to this second commodity jurisdiction request, the Department, by letter dated October 5, 1993, advised plaintiff that the request included cryptographic source code for data encryption, which is designated as a defense article under USML Category XIII((b)(1), and that a license would be required prior to its exportation from the United States. Tab 18. As stated below, the Department, on June 29, 1995, clarified that its CJ determinations concerned solely the Snuffle software.

D. Appeal of CJ Determinations

12. First CJ-191-92: Attached as Exhibit C to the Complaint is a letter dated September 22, 1993, which purports to be a letter to Ambassador Michael Newlin, then-Acting Deputy Assistant Secretary in the Bureau of Political-Military Affairs, appealing the Department's first commodity jurisdiction determination (CJ-191-92). The State Department searched its files at the Office of Defense Trade Controls associated with Dr. Bernstein's CJ requests, as well as our general correspondence and registration databases. Those files that would indicate the "tasking" of correspondence from the Office of the Assistant Secretary for Political-Military Affairs to ODTC were also searched. The Department also consulted with former Deputy

Assistant Secretary Michael Newlin as to whether he had received a copy of this appeal letter. A search was also conducted of the files of the current Deputy Assistant Secretary for Export Controls. Upon completion of these searches, the Department has not located any record of this appeal having been submitted.

13. Second CJ-214-93: Dr. Bernstein did not appeal the Department's determination for his second commodity jurisdiction request (CJ-214-93).

E. Basis of CJ Determination

14. On matters involving cryptographic devices and software, the National Security Agency ("NSA") provides to the State Department, on behalf of the Department of Defense, a technical evaluation of the commodity and recommends whether it is covered by Category XIII(b)(1) of the USML. NSA undertook a technical evaluation of the Snuffle software submitted by Dr. Bernstein and recommended that the State Department find that Snuffle is covered by Category XIII(b)(1) of the USML. The basis of NSA's technical evaluation is described in the Declaration of William P. Crowell, Deputy Director of the National Security Agency. Taking into account NSA's views in this matter, the State Department determined that the Snuffle software was covered by Category XIII(b)(1) of the USML and subject to the ITAR.

15. On April 27, 1992, the Department announced a procedure for the expeditious transfer of jurisdiction from the State Department to the Commerce Department for "mass-market" cryptographic software products with encryption that meet specified criteria. Tab 20. NSA determined that Snuffle did not meet the criteria for mass-market software subject to transfer to the

jurisdiction of the Commerce Department (or fall within the exceptions for cryptographic software under to Category XIII(b)(1) of the USML). See Crowell Declaration ¶ 21.

E. Clarification of CJ Determination

16. By letter dated June 29, 1995, the State Department clarified the scope of its commodity jurisdiction determinations. Tab 21. The Department reaffirmed its determinations that Dr. Bernstein's Snuffle software is a defense article covered by Category XIII(b)(1) of the United States Munitions List. The Department clarified, however, that its determinations were made solely as to the software (DJBCJF-3 and 4), and did not encompass the explanatory materials submitted with the CJ requests (DJBCJF-2, 5, and 6). DJBCJF-2 is a description of his Snuffle encryption system. DJBCJF-5 contains instructions for using Snuffle to encrypt. DJBCJF-6 contains instructions for programming a computer to use Snuffle to encrypt communications. The Department advised Dr. Bernstein as to the status of the explanatory information as technical data under the ITAR. Tab 21.

17. The sole administrative actions taken by the State Department in this matter were the two commodity jurisdiction determinations described above. The Department's determination is that Snuffle 5.0 software (DJBCJF-3 and DJBCJF-4) is designated as a defense article covered by Category XIII(b)(1) of the United States Munitions List. This means that its exportation from the United States is subject to the licensing jurisdiction of the Department of State. Accordingly, Dr. Bernstein was advised that if he wished to export his software from the United States, he must first obtain a license from the State Department. Dr. Bernstein did not apply for

a license to export his Snuffle software. Other than the commodity jurisdiction procedure initiated by Dr. Bernstein, no other provision of the ITAR has been applied by the State Department to Dr. Bernstein. Specifically, as stated above, the Department did not treat Dr. Bernstein's commodity jurisdiction requests as a request to publish a "scientific paper," and did not determine that he must apply for a license in order to publish such a paper or discuss his software in an academic setting.

18. By letters dated May 3, 1996, and July 3, 1996, Dr. Bernstein, through counsel again requested clarification of the Department's letter of June 29, 1995, concerning the ITAR's treatment of his Snuffle software and technical data, as well as the status under the ITAR of Dr. Bernstein's plans to teach an upcoming undergraduate-level course on cryptography. Tabs 22 and 23. In connection with preparing this declaration, which explains our views on these issues, I also responded to Dr. Bernstein's further requests by letter dated July 25, 1996. Tab 24.

III. Publication of Scientific Information and Academic Exchanges Under the ITAR.

19. The ITAR's export controls are applicable to proposed exports of defense articles, defense services, and technical data by anyone in the United States. Because of this, concerns have been raised in the past that conveying information to foreign nationals in a university environment might constitute an export of technical data for which a license might be required.[4] While I have been the

[4] Technical data is defined to include information "which is required for the design[,] development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles." 22 C.F.R. § 120.10(a)(1).

Director of DTC only since November 1994, I understand that earlier indications that the government might regulate academic exchanges of information under the ITAR generated considerable debate in the late 1970s and early 1980s.

20. In response thereto, the State Department published revisions to the ITAR in December 1984 which specifically noted that concern had been expressed that the ITAR could be read in an overbroad manner to encompass exchanges of information in a purely academic setting. See *Revisions to International Traffic in Arms Regulations, Supplementary Information*, 49 Fed. Reg. 47683 (Dec. 6, 1984) (Tab 1B). The Department acknowledged these concerns and took steps to alleviate them. Since 1984, the ITAR has been amended in order to indicate more clearly that publicly available information and academic exchanges are not treated as technical data. Tabs 1C-1E.

21. Most notably, specifically exempted from the definition of technical data is "information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities," 22 C.F.R. § 120.10(a)(5), and information that is in the "public domain." Id. Information is in the "public domain" if it is published and generally available and accessible to the public through, for example, sales at newsstands and bookstores, subscriptions, second class mail, and libraries open to the public. 22 C.F.R. § 120.11. Information is also in the

---

This includes, for example, information in the form of blueprints, drawings, photographs, plans, instructions, or documentation. Id. It also includes classified information relating to defense articles and services. Id. § 120.10(a)(2).

public domain if it is made generally available to the public "through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States" or "through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community." 22 C.F.R. § 120.11(a)(6), (8).

22. The regulatory exemptions set forth above describe categories of information that are specifically excluded from the technical data definition. As the regulations provide, the State Department does not seek to regulate information which is available in the public domain through the various means set forth in the regulations described above. Moreover, the Department does not seek to regulate the means themselves by which information is placed in the public domain. The Department does not review in advance scientific information to determine whether it may be offered for sale at newsstands and bookstores, through subscriptions, second-class mail, or made available at libraries open to the public, or distributed at a conference or seminar in the United States. These clear examples are included in the ITAR to enable individuals to determine for themselves whether particular information is subject to the regulations as technical data. Indeed, individuals rarely -- if ever -- seek a determination from the Department as to whether information is in the public domain, and the regulations are not applied to establish a prepublication review requirement for the general publication of scientific information in the United States.

23. Similarly, the Department does not try to substitute its judgment for that of university or academic scholar in such matters as whether certain ideas constitute "general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities," 22 C.F.R. § 120.10(a)(5) or "fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community." 22 C.F.R. § 121.11(8). Rather, the specific mention of these exemptions in the ITAR is intended as an assurance to the academic community as to the general non-applicability of the ITAR to a university setting -- and not for the purpose of establishing a role for the Department in regulating scientific publication, academic exchanges or information, or fundamental research in the United States. Examples of scientific research on cryptologic theories published in academic journals and discussed at academic symposia are attached to the Declaration of William P. Crowell of the National Security Agency. See Crowell Decl. ¶¶ 22-32 and Tabs 1-10. The State Department does not require a person to obtain a license to merely publish or discuss such scientific papers concerning cryptographic theories or algorithms.

24. In sum, an individual who wishes merely to publish a scientific paper, or to discuss scientific theories in an academic setting, is not thereby required to apply to the State Department for a license. The Department did not require this of Dr. Bernstein in response to his own commodity jurisdiction requests, and does not apply the ITAR in this manner.

25. In addition to the specific regulatory exceptions to the definition of technical data, the Department also indicated in December 1984, in response to concerns that the ITAR might reach academic discussion, that it intends to interpret the ITAR in a manner described by the court in United States v. Edler Industries, 579 F.2d 516, 521 (9th Cir. 1978). See 49 Fed. Reg. 47683 (Dec. 6, 1984) (Tab 1B). In accordance with Edler, the Department's practice is to regulate technical data if it is "significantly and directly related to specific articles on the Munitions List," and is to be exported in connection with "the provision of technical assistance for the foreign manufacture of articles that, if manufactured domestically, would be on the Munitions List," i.e., "the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise." Edler, 579 F.2d at 521.

26. Consistent with Edler, the Department licenses the export of technical data in two general contexts: first, if such an export would constitute a "defense service," that is, the actual provision of technical assistance and training by a U.S. person to a foreign person in the design, development, engineering, manufacture, production, assembly testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles on the USML, see 22 C.F.R. § 120.9(a)(1); or, second, if the export of technical data is directly related to a defense article and is intended to assist a foreign entity in obtaining, maintaining, repairing, or operating that article. These are the circumstances in which requests for technical data licenses typically arise. Thus, a key element of the Department's controls on the export of technical data is not simply the status of the

information at issue, but the specific conduct intended by the exporter. If, by the export of technical data, an individual intends to provide technical assistance to a foreign person in the maintenance or use of a defense article, or is providing information to a foreign entity with the intent to aid in the development or use of the article, a license would be required.

27. It is important to note as well that the technical data for which export licenses are sought normally has not been placed in the public domain by the exporter, for example because it might constitute information classified by the government, or legally controlled pursuant to a defense contract, or privileged and proprietary commercial information specifically developed by the exporter in connection with a defense article. Most requestors seeking to export technical data come to the Department for a license because the information at issue is proprietary or classified, and because they seek to export it specifically in connection with the provision of a defense service or to assist a foreign entity in obtaining or maintaining a defense article.

28. In sum, the ITAR seeks to exclude from export controls information which already is readily available to the public and, instead, focuses on controlling the export of information that is not publicly available and which is sought to be exported in connection with a defense service or technical assistance.

29. This is not to say that the export licensing requirements of the ITAR concerning technical data might never be applicable to those who work in a university or academic setting. A professor, like everyone else, would have to obtain a license in order to provide, in a private capacity, technical assistance to foreign

persons, or information for the purpose of assisting a foreign entity in obtaining, maintaining, or using a Munitions List item. A major university that runs an essentially commercial facility that develops or manufactures a Munitions List item where foreign persons are employed is also subject to the ITAR.[5]

30. Accordingly, the Department has advised Dr. Bernstein that, consistent with Edler, if his objective or intent in exporting technical data were to furnish technical assistance to a foreign person or enterprise in obtaining or developing cryptographic software, a license would be required. However, absent such an intent or conduct of this nature, the Department has also advised Dr. Bernstein that the mere "publication or teaching" of technical data concerning Snuffle 5.0 software would not violate the ITAR. Tab 24.

IV. Regulation of Cryptographic Software Under the ITAR

31. The ITAR's controls on cryptographic software are distinct from those concerning technical data. A license is required before cryptographic software can be exported. See 22 C.F.R. § 121.1 XIII(b)(1). However, the State Department does not regulate the export of cryptographic software on the basis of the content of any scientific theory (or other ideas) that are implicit in the software. Nor is cryptographic software controlled under the ITAR on the basis of whether or not the export is intended to convey a

---

[5] Even in this context, the ITAR contains an exception to technical data licensing controls setting forth circumstances under which disclosures of unclassified technical data in the United States by U.S. institutions of higher learning to foreign persons who are in their full-time and regular employment are not regulated. 22 C.F.R. § 125.4(b)(10).

scientific theory. In this case, the Department did not require Dr. Bernstein to apply for a license to export his software for the purpose of regulating his idea in developing Snuffle. Nor was Dr. Bernstein's intent to communicate an idea or theory at all a factor in our decision. (As noted, the item describing the scientific idea behind the Snuffle Encryption System [DJBCJF-2] is not subject to the ITAR.)

32. Rather, cryptographic software is covered on the United States Munitions List where it has "the capability of maintaining secrecy or confidentiality of information." 22 C.F.R. § 121.1, XIII(b)(1). It is the function of the software that brings it within Category XIII(b)(1), and on this point the Department seeks the technical advice of NSA. Cryptographic products and software that do not function to maintain the general secrecy of information, are specifically excluded from Category XIII(b)(1), such as for a data authentication and access control functions, or for banking-related transactions. 22 C.F.R. § 121.1, XIII(b)(1)(ii),(v),(vi). In addition, software that meets certain "mass-market" and specific encryption criteria can be transferred to the jurisdiction of the Commerce Department. 22 C.F.R. § 121.1, Category XIII(b)(1) (note) and Tab 20.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 2/25/96

WILLIAM J. LOWELL

ORIGINAL

FRANK W. HUNGER
Assistant Attorney General
MICHAEL J. YAMAGUCHI
United States Attorney
MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198
VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460

Attorneys for the Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN, Plaintiff, v. UNITED STATES DEPARTMENT OF STATE, et al., Defendants.	C 95-0582 MHP **MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT.** Hearing: September 20, 1996 Time: 12:00 Noon Judge Marilyn Hall Patel

particular publication can be placed in the public domain. See Compl. ¶ 141, 156 (claiming information not already in the public domain can be placed there). This is not how the regulations are applied, nor a reasonable reading of the provisions at issue.

In fact, the State Department does not seek to control the various means by which information is placed in the public domain. Lowell Decl. ¶ 22. The Department does not review scientific information to determine whether it may be offered for sale at newsstands and bookstores, through subscriptions, second-class mail, or made available at libraries, or distributed at a conference or seminar in the United States. Id.

> These clear examples are included in the ITAR to enable individuals to determine for themselves whether particular information is subject to regulation as technical data. Indeed, individuals rarely -- if ever -- seek a determination from the Department as to whether information is in the public domain, and the regulations are not applied to establish a prepublication review requirement for the general publication of scientific information in the United States.

Id.

Similarly, the State Department does not try to substitute its judgment for that of a university or academic scholars as to whether certain ideas constitute general scientific of mathematical principles commonly taught in colleges and universities, 22 C.F.R. § 120.10(a)(5) or fundamental research in science at institutions of higher learning in the United States. Id. § 121.11(a)(8). Lowell Decl. ¶ 23.

> Rather, the specific mention of these exemptions in the ITAR is intended as an assurance to the academic community as to the general non-applicability of the ITAR to a university setting -- and not for the purpose of establishing a role for the Department in regulating scientific publication, academic exchanges of information, or fundamental research in the United States.

Id.

Dr. Bernstein's assertion that all scientific speech about cryptology is excluded from the definition of what could be in the public domain, Compl. ¶ 157, is belied by a wealth of academic exchanges and conferences that routinely occur in the field of cryptology. See Declaration of William P. Crowell of the National Security Agency, ¶¶ 22-32 and Tabs 1 to

newsletters setting forth information on the CJ procedures. See Tab 2 to Lowell Declaration.

CONCLUSION

For the foregoing reasons, defendants' motion for summary judgment should be granted.

Respectfully Submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198

By MB Uitti Per Telephone Authorization
Anthony J. Coppolino

VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460

Attorneys for the Defendants

ORIGINAL

FRANK W. HUNGER
Assistant Attorney General
MICHAEL J. YAMAGUCHI
United States Attorney
MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198
VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460

Attorneys for the Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO HEADQUARTERS

DANIEL J. BERNSTEIN, Plaintiff, v. UNITED STATES DEPARTMENT OF STATE, et al., Defendants.	C 95-0582 MHP **DEFENDANTS' OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AND IN FURTHER SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** Hearing: September 20, 1996 Time: 12:00 Noon Judge Marilyn Hall Patel

commonly taught in schools, colleges and universities or information that is in the public domain." 22 C.F.R. § 120.10(a)(5). Information in the "public domain" includes information publicly available through unlimited distribution at a conference in the United States generally accessible to the public, and through fundamental research in science and engineering at institutions of higher learning in the United States that is ordinarily published and shared broadly in the scientific community. 22 C.F.R. § 120.11(a)(6), (8).

Moreover, the regulations are not applied to regulate the means by which such information is placed in the public domain. Def. Mem. at 7-8; Lowell Decl. ¶ 22-23. Rather, consistent with Edler, ITAR controls on technical data are applied to regulate the export of non-public, proprietary or classified information sought to be disclosed to a foreign person or entity in connection with a defense service (technical assistance and training) or the development or maintenance of a defense article. Id. ¶ 26-27. This is the typical scenario in which parties seek to export technical data, not academics applying for a license to publish their ideas.[9]

For these reasons, plaintiff's claim that all disclosures of scientific information on cryptography in the United States constitutes an export of technical data, since inevitably a foreign person might receive it in class or through publication, is wrong. Even more so than the provisions at issue in Edler, the ITAR can readily be construed to carve out from regulation basic First Amendment activities.[10]

---

[9] Plaintiff's contention that information exempt from technical data provisions through the public domain exception is nonetheless "recontrolled" as a "defense service," Pl. Mem. at 7, n.12, misses a key distinction which the court of appeals has twice recognized. Information in the public domain is not technical data subject to export controls. However, providing technical assistance to a foreign entity with the intent to aid, inter alia, the design, development, operation, or maintenance of a munition, even through the use of publicly available information, is conduct that the government can control consistent with the First Amendment. Edler, 570 F.2d at 522; United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989).

[10] Plaintiff's reliance on a 1981 memorandum from the Office of Legal Counsel of the Department of Justice ("OLC"), Pl. Mem. at 13, is misplaced. OLC's analysis was quite similar to the court's in Edler, which the State Department stated in 1984 it would

in connection therewith (defense services). While such controls may be cross-referenced in the regulations, there are distinct regulatory provisions for each including, of most pertinence, a separate definition of technical data with its various exceptions.

3. The Exemptions To The Definition Of Technical Data Are Not Vague.

Plaintiff challenges as vague the very exceptions that exclude a host of information from export controls. These exemptions are far from vague. Plaintiff claims first that the exception for "scientific, mathematical, and engineering principles commonly taught in schools, colleges and universities" is vague, based solely on the notion that one school might not teach what another does. Pl. Mem. at 35. This argument can be quickly passed over. The ITAR does not purport to require uniformity in what schools teach. The obvious purpose of the exception is to indicate that technical data does not include information exchanged in the common, everyday occurrence of a university lecture. The ITAR does not indicate that the government must pass judgment on what can or cannot be deemed a "common" academic principle, nor is it so applied. Lowell Decl. ¶ 23.

Plaintiff's attack on the "public domain" exemption is also meritless. That provision contains several specific exceptions as to what is controlled as technical that any ordinary person can understand -- information in bookstores, newsstands, or disclosed at conferences. Plaintiff sees a "Catch-22" "lurking" in the provision that, unless something is already published, it is subject to export controls. He would construe the definition to mean, in other words, that nothing can be published without the government's approval. Not only is this wrong as a factual matter, see Lowell Decl. ¶ 22, it is by far the most un-reasonable interpretation of the provision, one that people of ordinary intelligence are least likely to assume is the case.[32]

---

[32] Plaintiff's discussion of the public domain provision is also highly confusing. He claims that "software" should be treated as in the public domain because that exception refers to "information," not "technical data." Pl. Mem. at 35-36. The public domain provision is a clear and express exception to the definition of "technical data." 22 C.F.R. § 120.10(a)(4) (technical data does "not include . . .information in the public

more than inform, but has a practical use -- in the case of Snuffle to provide for zero-delay encrypted conversations. Moreover, what plaintiff seeks to do is not merely "publish ideas" but export, without limitation to anywhere in the world, a commodity that he and his declarants have explained has a practical cryptographic function. To describe this merely as "publishing" an "idea" is disingenuous. The government's action is fully consistent with how Edler and several other courts, see Def. Mem. at 20, have upheld the application of export controls to matters that have national security and foreign policy significance.

CONCLUSION

For the foregoing reasons, defendants' motion for summary judgment should be granted, plaintiff's motion for summary judgment should be denied, and this action should be dismissed with prejudice.

Respectfully Submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198

by MB Uitti
Anthony J. Coppolino

VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460

Attorneys for the Defendants

FRANK W. HUNGER
Assistant Attorney General
MICHAEL J. YAMAGUCHI
United States Attorney
MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198
VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460

Attorneys for the Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO HEADQUARTERS

DANIEL J. BERNSTEIN, Plaintiff, v. UNITED STATES DEPARTMENT OF STATE, et al., Defendants.	C 95-0582 MHP **DEFENDANTS' OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AND IN FURTHER SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** Hearing: September 20, 1996 Time: 12:00 Noon Judge Marilyn Hall Patel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTRODUCTION

It is difficult enough to litigate a case where there is some common understanding between the parties as to the nature of the dispute at issue. But this case is unnecessarily complicated by the plaintiff, who makes the unfounded assertion that the government "requires a private citizen to submit his ideas . . . for review and licensing prior to publication or public discussion," and that it "uses such a process to censor publication of ideas about an entire area, namely the science of cryptography." Pl. Mem. at 1.

Such a characterization of the matters at issue in this case is profoundly in error. The evidence on the record demonstrates that there is a broad, dynamic exchange of academic ideas and scientific publication in the field of cryptography -- textbooks, articles, symposia, and fundamental research that include discussions of cryptographic algorithms and their theory.[1] The government does not require that academics submit their "ideas" for review before they can be "published" or discussed in a classroom. Yet plaintiff repeats this unsupported assertion throughout his argument, to the point where it often substitutes for legal analysis itself. In effect, plaintiff starts with the assumption that the government bans all speech on cryptography, then argues that the First Amendment is thereby violated.

If plaintiff were claiming solely that his "Snuffle" cryptographic source code constitutes the "academic idea" at issue, and were challenging restrictions on his right to disseminate it abroad, this case would be fairly straightforward one. The Court could look to the nature of cryptographic source code, the regulations at issue, apply appropriate First Amendment law, and decide the matter. Instead, plaintiff goes far afield, bringing broad facial challenges that seek to invalidate the ITAR as to all applications, by claiming that controls on the export of technical data are used to censor the "publication" of all "ideas" in this field. What is more, plaintiff does not merely assert that the regulations could be "construed" this way, but claims that this actually occurs.

This is easily shown to be erroneous and, hence, there is no genuine issue of material

---

[1] Indeed, plaintiff himself cites articles describing the theory of cryptographic source code, see Declaration of Daniel J. Bernstein ¶ 15, and agrees that cryptographic algorithms are regularly published for peer review.

fact presented by this claim. What is left for the Court to assess is a theoretical legal question as to whether the regulations so vague on their face that they might be construed to apply to academic exchange and scientific publication. As defendants have shown, the regulations contain express exemptions for basic First Amendment activities such as publication, teaching, fundamental research, and symposia discussion, and hence are readily susceptible to a facial construction that is consistent with First Amendment freedoms.

The real issue in this case is whether export licensing controls on one specific element that the Court has found constitutes speech -- cryptographic source code -- violates the First Amendment.[2] On this claim, no genuine issue of material fact is presented as well. There is no dispute that the government does regulate the export of cryptographic software, including source code, and no dispute that plaintiff was advised that the export of his cryptographic software was subject to licensing controls. The legal issue is whether such controls impermissibly regulate speech.

As defendants demonstrate, such software is not regulated to suppress the content of any ideas, but to control the spread world-wide of a commodity that can be utilized to encrypt information on a computer, and thereby harm sensitive national security and foreign policy objectives served by foreign intelligence collection activities. Indeed, plaintiff's submission presents considerable evidence that supports the government's position. In terms quite similar to that set forth by NSA Deputy Director Crowell, plaintiff's submission explains how cryptographic software functions to encrypt information on a computer system. See, e.g., Declaration of Bruce Schneier ¶ 2 ("[t]he aim of encryption is to turn an otherwise intelligible message into gibberish so that a person who intercepts it cannot read it") and ¶ 15 ("[c]ryptography is well-suited for computers" and "[t]oday almost all cryptography is done by computers and dedicated computer chips"); see also Declaration of Michael Paul Johnson ¶ 19 (source code is compiled "simply by pressing a button" to achieve a "working

---

[2] Bernstein v. Department of State, 922 F. Supp. 1426, 1439 (N.D. Cal. 1996) (making the sole substantive holding that source code is speech for First Amendment purposes).

program"). Thus, even assuming the principal point made in plaintiff's motion, that "programming language" is a means of exchanging ideas among academics who can understand it, Pl. Mem. at 3-4, plaintiff concedes perhaps the most critical point defendants make. cryptographic source code is a computer program that can be utilized to encrypt information. Once this fact is established -- and it is not reasonably controverted -- the conclusion readily follows that such software is not regulated to limit the content or artistic merit of its programming language, but rather because of what such a "working program" can do -- encrypt information on a computer.

Plaintiff's assertion that strict scrutiny applies to export controls on cryptographic software is wrong. Plaintiff simply does not show that the government regulates such software for its speech value or content. The essence of his claim that content is regulated is that the government seeks to appraise the "possible uses, strength and effectiveness" of such software. See Pl. Mem. at 29. The government does evaluate the capability of cryptographic software to "maintain the secrecy of information" in deciding whether it is subject to export controls. 22 C.F.R. § 121.1, XIII(b)(1). But this is not an evaluation of the content of speech, such as the theories or ideas underlying the software, but of the functionality of the program. Indeed, such a capability would be assessed for all cryptographic products and software, including object code and hardware devices. As shown below, intermediate First Amendment scrutiny applies in evaluating such export controls, and the policy readily survives under such review. None of plaintiff's factual assertions or submissions present a "genuine issue of material fact" that would preclude summary judgment on all claims for the defendants. Anderson v. Liberty Lobby, 477 U.S. 242, 255 (1986).[3]

---

[3] Plaintiff styles his motion as both for "summary adjudication" on whether "strict scrutiny" applies to ITAR controls, and "summary judgment" on his vagueness and overbreadth claims. To the extent plaintiff is invoking Fed.R.Civ.P. 56(d), "summary adjudication" applies where summary judgment under Rule 56 is not rendered on the whole case. The rule requires the court to ascertain which "facts exist without substantial controversy" and to specify them in order to limit genuine factual issues for trial. "There is no such thing as an independent motion under Rule 56(d)." Arado v. General Fire

FACTUAL BACKGROUND

In his "STATEMENT OF FACTS," plaintiff avers that the "Defendants have told plaintiff that he cannot present his ideas." Pl. Mem. at 3. This assertion goes beyond reasonable advocacy. Plaintiff cannot point to anything in the record indicating that defendants said anything so sweeping. In fact, what plaintiff sought from the government by letter dated June 30, 1992, was a "commodity jurisdiction determination" for his software, Snuffle 5.0, which he stated that he wished to export. See Tab 3 to Lowell Declaration. Plaintiff went on to describe the cryptographic function of this software as a "zero-delay, private key, encryption system." Id.

The State Department's first CJ determination specifically referenced "Snuffle 5.0 software." Tab 4 to Lowell Declaration. This determination did not indicate that plaintiff was barred from publishing or discussing ideas concerning his software without a license. It indicated that Snuffle 5.0 was covered by Category XIII(b) of the United States Munitions List, and that a license would be required before it could be exported from the United States. Id. It is plaintiff who has construed this to mean he is not free to "publish his ideas."

Plaintiff submitted a second CJ request on July 15, 1993, in which he lumped together the Snuffle software (DJBCJF-3 and 4), with a "paper" describing the software (DJBCJF-2), and instructions on how to make it operational on a computer (DJBCJF-5 and 6). See Lowell Decl. ¶ 16. Plaintiff avers that he "sought to give Defendants the opportunity to consider each item separately." Pl. Mem. at 8. He also states that his "main purpose in submitting separate requests was to see whether the Government would designate my mathematical description per se as a defense article." Bernstein Decl. ¶ 35.

Extinguisher Corp., 626 F. Supp. 506 (N.D. Ill. 1985). The rule's issue-narrowing provision operates only in the wake of an unsuccessful motion for summary judgment under Rule 56(a) or 56(b). Id. at 509. Moreover, this rule is concerned with factual matters that do not present a genuine issue for trial, not fundamental legal questions in dispute, such as whether "strict scrutiny" is the appropriate standard of review. Plaintiff's entire motion should be treated as one for summary judgment.

These self-serving characterizations are unsupported in the record. In fact, plaintiff did not separately describe his "paper" or "instructions" on how to use Snuffle. Rather, he described every item submitted as if it were cryptographic software, i.e., "originally designed to convert any one-way hash function into a zero-delay private-key encryption system." See Tab 16 to Lowell Declaration. If his "main purpose" was to get an evaluation solely of his mathematical idea, this was not made reasonably clear.

In the State Department's second CJ determination dated October 5, 1993, plaintiff was advised that the referenced items "contain cryptographic source code for data encryption," Tab 18 to Lowell Declaration, -- again a reference to the Snuffle source code itself. Plaintiff was not told that he was precluded from "publishing ideas" about his software, only that the software was included on the USML and subject to export licensing controls. Id.

Any confusion or dispute over how the ITAR was applied to plaintiff should be well behind the parties, since the government has long since clarified the matter. After plaintiff filed suit claiming he was barred from "publishing a paper" on his ideas, the State Department, on June 29, 1995, further explained the basis of its determinations.[4] Defendants explained that the determination designated plaintiff's Snuffle software (DJBCJF 3 and 4) as a defense article subject to export controls, not his "paper" (DJBCJF-2), or instructions explaining how to use Snuffle on a computer (DJBCJF-5 and 6). Lowell Decl. ¶ 16.[5]

The Court appears to have recognized what happened here. In resolving defendants'

---

[4] There was nothing inappropriate about this effort at clarification. This letter was prepared at the end of the Court-mandated meet-and-confer process, which presumably is intended to narrow issues in dispute and present the Court with a limited controversy. Moreover, plaintiff never exhausted administrative remedies for the second CJ determination and, in the absence of such an administrative record, defendants sought to clarify for the Court the intent of its administrative actions.

[5] Indeed, those requesting a commodity jurisdiction determination are required to submit explanatory information for the commodity, 22 C.F.R. § 120.4(c), and NSA did not separately evaluate these items for export control purposes. Crowell Decl. ¶ 16.

motion to dismiss, it indicated that plaintiff's claims with respect to his scientific paper (DJBCJF-2) appeared to be moot, and that a prior restraint claim concerning his technical data (DJBCJF-5 and 6) was foreclosed by United States v. Edler Industries, 579 F.2d 516, 521 (9th Cir. 1978). See Bernstein v. Department of State, 922 F. Supp. at 1434 n.12 and 1438 n.20. Yet plaintiff challenges the Court's decision, arguing that "voluntarily ceas[ing]" to restrain publication of an "obvious speech item" cannot create mootness. Pl. Mem. at 10, n.21. This is specious.

The CJ determinations referenced "Snuffle 5.0" and "cryptographic source code for data encryption," and did not purport to restrain the "publication" of any ideas. Plaintiff appears reluctant to take at least a partial "yes" for an answer that the determination was limited to his source code, because it undermines his legal theories that the government, through the ITAR, seeks to regulate scientific publication. He has yet to offer a plausible reason why the State Department would purport to regulate his scant, one-page description of Snuffle (DBJCJF-2), while detailed discussions of cryptographic theories and algorithms are broadly published without regulation. See Tabs 1-9 to Crowell Declaration. Particularly where defendants have clarified the matter again by letter dated July 25, 1996, see Tab 24 to Lowell Declaration, and have fully set forth their regulatory practice, there is no basis for the Court to revisit the treatment of plaintiff's submissions.

What is not in dispute in this case is that Snuffle 5.0 is subject to export licensing controls, and such cryptographic source code can function to maintain the secrecy of information on a computer system. Plaintiff claims that he wrote his source code -- a cryptographic algorithm for scrambling and descrambling communications set forth in computer programming language -- in order to express his idea "as precisely as possible." Pl. Mem. at 3. He avers that algorithms are written in programming language "'for people to read as much as they are written for machines to execute.'" Pl. Mem. at 3 (quoting Ableson and Sussman, *Structure and Interpretation of Computer Programs* (1985)). Plaintiff also avers that "'[l]iterature of the program genre is performable by machines, but that is not its main purpose." Id. at 4 (quoting Knuth, *Literate Programming*, IX).

As set forth below, even if computer programs are meant to be read by those who can understand programming language, this is not material to the legal questions before the Court. The underlying purpose of export controls on cryptographic source code is not concerned with their "literary" value, but the fact that such programs are "for machines to execute" on a computer. In other words, even if expressing cryptographic algorithms in programming language is informative to some academics, that does not mean the government violates the First Amendment by regulating its export because, as plaintiff concedes, such software also has a functional value.[6]

ARGUMENT[7]

As defendants' have noted, plaintiff's multiple claims present just two basic issues. First, do ITAR controls on the export of technical data regulate academic discussion and constitute a system of prior restraint on the publication of scientific information? Second, do ITAR controls on the export of cryptographic software impermissibly regulate the content of speech? See Def. Mem. at 4-5. Plaintiff intermixes argument on both issues. He claims the ITAR's technical data provisions bar disclosure of his ideas in the United States in any manner, either through publication or in the classroom, because they would "inevitably be disclosed to a foreign person." Pl. Mem. at 9. This contention is without merit. The ITAR, on its face and as applied, does not regulate mere academic exchanges or the publication of scientific ideas on cryptography as an export of technical data. Def. Mem. at 5-14.

Plaintiff also claims that "he may not take or send Snuffle 5.0 source code outside of

---

[6] At the end of his statement of facts, plaintiff raises a new aspect of his claim -- namely whether the ITAR reaches his ability to teach a class at the University of Illinois starting in January. Pl. Mem. at 4. The government has never determined that plaintiff must obtain a license before teaching a class on cryptography. Hence, this allegation is not at issue in this case. Even if it were considered, the government has advised plaintiff that academic teaching concerning cryptography is not subject to ITAR controls. See Tab 24 to Lowell Declaration.

[7] Defendants have set forth the relevant Statutory Background in our prior memorandum, see Def. Mem. at 2-3, and will respond to plaintiff's regulatory interpretations in connection with his vagueness claims.

the United States in any manner." Pl. Mem. at 9. This too is wrong, though closer to the issue at hand. While cryptographic software is subject to export licensing controls, this does not mean, however, that it can never be exported -- only that a license is required beforehand so that the government may assess its security implications, including its intended end-use and end-user. See Lowell Decl. ¶ 5. By challenging this, plaintiff appears to seek the right export his software anywhere in the world, in the name of "academic freedom," without concern as to which foreign person or entity may obtain it and how they may use it.

I. ITAR CONTROLS ON THE EXPORT OF TECHNICAL DATA DO NOT REGULATE ACADEMIC DISCUSSION OR THE PUBLICATION OF IDEAS.

A. The Technical Data Provisions Do Not Impose a System of Prior Restraint on Speech.

The technical data provisions of the ITAR regulate information related to defense articles, such as "blueprints, drawings, plans, instructions, and documentation," as plaintiff notes. Pl. Mem. at 11 (citing 22 C.F.R. § 120.10(a)(1)). Starting from this premise, plaintiff reaches an unwarranted conclusion -- that all disclosures of scientific information, through academia or publication, are subject to export licensing controls, because "exporting" technical data includes disclosure to a foreign persons in the United States. This is plaintiff's own theoretical speculation as to what the ITAR could conceivably encompass. The question is whether the regulations, viewed as a whole, are susceptible to an interpretation that does not impermissibly limit academic and scientific exchange. This involves at least two considerations: (i) whether the regulations themselves seek to limit the reach of the technical data definition and, hence, controls on its export; and (ii) how the government actually applies the definition in regulatory practice.[8]

Defendants have largely set forth our analysis already. The ITAR itself exempts from the definition of technical data a broad array of information. See Def. Mem. at 7. This includes "information concerning general scientific, mathematical or engineering principles

[8] Since the ITAR was not applied to restrain publication of plaintiff's paper here, defendants assess this as a facial vagueness claim.

commonly taught in schools, colleges and universities or information that is in the public domain." 22 C.F.R. § 120.10(a)(5). Information in the "public domain" includes information publicly available through unlimited distribution at a conference in the United States generally accessible to the public, and through fundamental research in science and engineering at institutions of higher learning in the United States that is ordinarily published and shared broadly in the scientific community. 22 C.F.R. § 120.11(a)(6), (8).

Moreover, the regulations are not applied to regulate the means by which such information is placed in the public domain. Def. Mem. at 7-8; Lowell Decl. ¶ 22-23. Rather, consistent with Edler, ITAR controls on technical data are applied to regulate the export of non-public, proprietary or classified information sought to be disclosed to a foreign person or entity in connection with a defense service (technical assistance and training) or the development or maintenance of a defense article. Id. ¶ 26-27. This is the typical scenario in which parties seek to export technical data, not academics applying for a license to publish their ideas.[9]

For these reasons, plaintiff's claim that all disclosures of scientific information on cryptography in the United States constitutes an export of technical data, since inevitably a foreign person might receive it in class or through publication, is wrong. Even more so than the provisions at issue in Edler, the ITAR can readily be construed to carve out from regulation basic First Amendment activities.[10]

---

[9] Plaintiff's contention that information exempt from technical data provisions through the public domain exception is nonetheless "recontrolled" as a "defense service," Pl. Mem. at 7, n.12, misses a key distinction which the court of appeals has twice recognized. Information in the public domain is not technical data subject to export controls. However, providing technical assistance to a foreign entity with the intent to aid, inter alia, the design, development, operation, or maintenance of a munition, even through the use of publicly available information, is conduct that the government can control consistent with the First Amendment. Edler, 570 F.2d at 522; United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989).

[10] Plaintiff's reliance on a 1981 memorandum from the Office of Legal Counsel of the Department of Justice ("OLC"), Pl. Mem. at 13, is misplaced. OLC's analysis was quite similar to the court's in Edler, which the State Department stated in 1984 it would

Beyond this, the Court can readily take notice that academic teaching, publication, research, and symposia concerning cryptography routinely occur in the United States. See Crowell Declaration, ¶¶ 23-31; Tabs 1-9. Plaintiff himself provides additional examples of such published research on cryptography and cryptographic algorithms. For example, Dr. Bernstein refers to two articles that discuss the use of hash functions for encryption. Declaration of Daniel J. Bernstein ¶ 15.[11] Plaintiff also notes, as defendants have, that cryptographic algorithms are normally published and tested. Id. ¶ 52; see Crowell Decl. ¶ 22. In addition, Dr. Abelson notes that his book on computer programming is used in courses at over 200 colleges and universities world wide, courses that presumably provide skills on how to program and compile source code. Declaration of Harold Abelson ¶¶ 4-5.[12]

The distinction at issue is between presenting scientific theories or principles concerning cryptography in an article or the classroom, and sending actual cryptographic source code out of the country. Plaintiff is free "to teach about cryptography by teaching about the development and analysis of cryptographic computer programs." Pl. Mem. at 13. What plaintiff seeks is materially different. In the name of "academic freedom," he seeks the unfettered ability to export actual source code software -- a product that, unlike a magazine article or book discussing algorithmic theories, can readily be compiled and used to encrypt information on a computer -- including through transmission all over the world on the Internet

---

follow. See *Revisions to International Traffic in Arms Regulations, Supplementary Information*, 49 Fed. Reg. 47683 (Dec. 6, 1984) (Tab 1B to Lowell Declaration). What is more, as detailed in our opening memorandum, the ITAR has been amended multiple times, starting in December 1984, a few months after the last OLC opinion, to take better account of First Amendment concerns. See Def. Mem. at 12-14.

[11] Copies of these articles were located by defendants and are attached at Tabs 1 and 2 to the Declaration of Anthony J. Coppolino. Plaintiff submits other articles discussing algorithms, see Declaration of Carl M. Ellison, Exhibits A to D, although these do not appear to concern cryptographic algorithms.

[12] Defendants located this textbook and submit its Table of Contents at Tab 3 to the Coppolino Declaration. See, e.g., Chapter 5, § 5.3 on Compiling.

where it might be downloaded and used to encrypt information. This involves much more than the publication of ideas or teaching theory to a class.

For the foregoing reasons, the authority on which plaintiff relies to show the importance of academic freedom is therefore inapposite.[13] Plaintiff cites no case that supports the proposition that his right to academic freedom includes the right to transmit throughout the world a software product that can conceal communications on a computer, merely because he wishes to spread his "ideas" in this form. Plaintiff's reliance on the Pentagon Papers case, New York Times Co. v. United States, 403 U.S. 713 (1971), is likewise inapposite. There, the government sought to prevent *The New York Times* from publishing classified governmental reports on the Vietnam War. Here, the government does not use the ITAR to suppress publication of ideas on policy matters, controversial or otherwise. Nor does the government seek to suppress scientific exchange on cryptography, even though knowledge in this area may have national security implications for intelligence gathering as well as for maintaining computer security.

B. Freedman v. Maryland And Related Authority Is Inapposite.

Plaintiff's reliance on Freedman v. Maryland, 380 U.S. 51 (1964), and related authority, is also misplaced. Freedman concerned how the government could maintain a permissible system of prior restraint on potentially obscene materials, which are subject to no constitutional protection. The Supreme Court held that such a system must place the burden of proving the expression unprotected on the censor, limit the restraint to the shortest period of time compatible with judicial procedure, and assure prompt final judicial determination of

---

[13] See Regents of the University of California v. Bakke, 438 U.S. 265 (1977) (academic freedom generally includes right of university to select diverse student body); Keyishian v. Board of Regents, 385 U.S. 589 (1966) (striking down anti-subversive law as applied to faculty at state universities); Sweezy v. New Hampshire, 354 U.S. 234 (1956) (university faculty member's right to due process violated when he was investigated about the communist and subversive nature of his teaching).

obscenity. 380 U.S. at 58-59.[14] Freedman is inapposite because the ITAR, on its face, as applied by the State Department, and as construed by the court of appeals in Edler, does not purport to be a system for licensing the publication or dissemination of scientific speech.[15]

Plaintiff also cites authority that governmental licensing schemes affecting the dissemination of speech must set forth narrowly drawn, reasonable, and definite standards that limit administrative discretion in deciding when to permit speech to occur. See Forsythe County, Georgia v. Nationalist Movement, 505 U.S. 123 (1991) (invalidating ordinance granting city discretion to decide fee for parade without any limiting criteria). All of the cases on which plaintiff relies present fact patterns quite dissimilar from this one, involving ordinances that openly sought to limit access to public property to engage in free speech, or attempts to regulate private assembly to do so, in the absence of any limiting criteria.[16] The

---

[14] Freedman has been applied to assess the constitutionality of ordinances regulating obscene material. See United States v. 2,000 Paper Back Books, 565 F.2d 566, 572 (9th Cir. 1977); Spokane Arcades Inc. v. Brockett, 631 F.2d 135, 138 (9th Cir. 1980), aff'd., Brockett v. Spokane Arcades, Inc., 472 U.S. 491 (1984).

[15] It is noteworthy how much of plaintiff's prior restraint analysis is essentially lifted from the 1978 decision of the Department of Justice, Office of Legal Counsel. Exhibit to Declaration of Lee Tien at 60074-60089 (OLC Memo dated May 11, 1978). At that time, OLC expressed concern that the ITAR could be applied as a system of prior restraint against public information concerning cryptography, citing, inter alia, Freedman. Id. at 60083. Since that time, however, the ITAR has been amended multiple times, Edler upheld the technical data provisions at issue, and the State Department has made clear its adherence to this approach.

[16] See Lovell v. City of Griffin, 303 U.S. 444, 450 (1937) (invalidating an ordinance under which individuals had to apply to the city manager for a license to distribute any literature in the city, with no limits on the discretion to grant or deny the license); Niemotko v. Maryland, 340 U.S. 268, 271-72 (1950) (invalidating denial of access to a public park to a Jehovah's Witnesses group to talk about the Bible, where there was no ordinance limiting the city's "practice" as to when access should be permitted; Staub v. City of Baxley, 355 U.S. 313, 322 (1957) (invalidating ordinance applied to bar individuals from meeting in private homes for the purpose of discussing whether to unionize, which vested sole discretion in the Mayor to decide how the meeting might affect the "general welfare" of the city); Shuttlesworth v. City of Birmingham, 394 U.S. 147, 150-51 (1968) (invalidating ordinance requiring permit for a parade as applied to stop a peaceful civil rights march, since it vested sole discretion in the city to decide

activities at issue in these cases are inherently expressive (distributing literature, reading the Bible in a park, meeting in a private home to discuss union activities, marching for civil rights, putting on a theatrical production, placing newspapers in public). In contrast, the ITAR is directed at controlling the spread of defense-related commodities and technology abroad, and cannot reasonably be compared to such direct regulations of inherently expressive activities. Assuming such authority does apply here, the ITAR provides several specific examples of publicly available information that is not subject to controls. 22 C.F.R. § 120.11 (bookstores, newsstands, symposia, conferences, mail delivery, fundamental research, and common academic principles). As such, it sets forth criteria that limits the implementation of technical data controls, and stands in stark contrast to the restrictions at issue in the authority on which plaintiff relies.[17]

---

whether the march was consistent with the public interest); Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546 (invalidating denial of access to a municipal auditorium for the musical "Hair" again based solely on the city's judgment as to the potentially "obscene" nature of the production); City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 757 (1987) (invalidating ordinance giving mayor complete discretion to decide whether newsracks can be placed on public property).

[17] Plaintiff also claims that several ITAR procedures -- the commodity jurisdiction, registration, and recordkeeping procedures -- are part of a system of prior restraint. Defendants have already addressed most of these claims. The CJ process is not mandatory in any way. See 22 C.F.R. § 120.4; Def. Mem. at 14, n.18. The registration process applies to those seeking to export defense articles. 22 C.F.R. § 122.1(a). Based on plaintiff's assertion that he might violate the ITAR in doing so, see Tab 12 to Lowell Declaration, the State Department advised him that he might have to register and sent him registration information. Id. at Tab 13; see Def. Mem. at 37. Plaintiff challenges for the first time another ITAR requirement to prepare a Shippers Export Declaration with the export of defense articles, 22 C.F.R. § 123.16(a), and a record of how the article was exported. These requirements are surely justified with respect to those who actually export defense articles or provide defense services, but would not apply to activities outside the scope of the ITAR. Hence plaintiff's claim that he is compelled to "keep a log of his academic work and specify with any developments or refinements were discussed," Pl. Mem. at 18, is meritless.

II. ITAR CONTROLS ON CRYPTOGRAPHIC SOFTWARE DO NOT IMPERMISSIBLY REGULATE THE CONTENT OF SPEECH.

A. Export Controls on Cryptographic Software Are Content-Neutral And Strict Scrutiny Does Not Apply.

The remaining issue in this case is whether ITAR controls on cryptographic software impermissibly restricts freedom of speech. Whether a governmental regulation is subject to strict or intermediate First Amendment scrutiny depends on whether the restriction at issue is content-neutral. See Def. Mem. at 15-18. Plaintiff suggests that the standard of review applicable here was largely resolved by the Court in deciding that source code is speech for First Amendment purposes. See Pl. Mem. at 25. That does not end the analysis, however, since some element of speech or expression is at issue in every case in which the First Amendment is applied.

Rather, as the Supreme Court instructs, the principal inquiry in determining content neutrality is whether the government has adopted a regulation of speech because of disagreement with the message it conveys. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (citing Clark v. Community for Creative Non-Violence, 468 U.S. 288, 295 (1984)) ("CCNV") (emphasis added); Turner Broadcasting System, Inc. v. FCC, 114 S.Ct. 2445, 2459 (1994). This is to be discerned from the actual terms of the regulations at issue, including whether their "manifest purpose" is to regulate the content of speech. Turner, 114 S.Ct. at 2461; see Ward, 491 U.S. at 791 (the government's purpose is the controlling issue). As this authority indicates, the law or regulation at issue must be directed at the substantive content of speech in order for strict scrutiny to apply.[18]

---

[18] Thus, for example, the Supreme Court has held that a law barring the distribution of literature on the basis of whether it concerns "controversial issues of public policy" is content-based. Consolidated Edison Co. v. Public Service Comm'n., 447 U.S. 530, 533, 537 (1979). Likewise, a law that regulates on the basis of whether words would "arouse anger, alarm, or resentment in others on the basis of race, color, creed, religion, or gender" is content-based. R.A.V. v. St. Paul, 505 U.S. 377, 380, 391 (1992). See also Sable Communications v. FCC, 492 U.S. 115, 126 (1989) (restriction on access to "indecent" communications, i.e., patently offensive depictions of sexual or excretory activities, is content-based). See Def. Mem. at 16, n.20

Plaintiff posits three reasons why the ITAR regulates the content of speech, none of which have merit. First, plaintiff claims that the ITAR "removes discussion on the entire topic of cryptography from the 'market place of ideas.'" Pl. Mem. at 23. This argument simply assumes its own conclusion that the content of all speech is banned by the regulations. As a factual matter, this is not correct, since there is broad academic discussion of cryptography in the marketplace of ideas. See, e.g., Crowell Declaration, Tabs 1-10. Moreover, while the ITAR regulates certain information as technical data, the purpose of these controls has been held not to be directed at the content of expression. Edler, 579 F.2d at 521 (technical data provisions regulate the conduct of providing technical assistance in the development of a munition). Indeed, the court in Edler appeared to apply intermediate scrutiny in evaluating such controls, observing that "'[G]eneral regulatory statutes, not intended to control the content of speech but incidentally limiting its unfettered exercise,'" have not been regarded as in violation of the First Amendment when "'justified by subordinating valid governmental interests.'" 579 F.2d at 520 (quoting Konigsberg v. State Bar, 366 U.S. 36, 50-51 (1961)). Hence, the mere fact that technical data is defined to include information is not dispositive of whether the regulation is content-based.[19]

Plaintiff next argues that defendants review cryptographic software in order to appraise its "possible uses, strengths, and effectiveness." Pl. Mem. at 23. The government does assess the use of the software to maintain the secrecy of information in deciding whether it is subject to export control under the USML. See 22 C.F.R. § 121.1, XIII(b)(1). But evaluating the function of a software product -- what it can do when installed on a computer -- does not constitutes a regulation of the content of ideas. Assessing such a function is undertaken for all cryptographic products covered by the USML, including hardware devices and object code, not merely for source code. Again, the dispositive issue is the underlying

---

[19] Plaintiff's reliance on Police Department of Chicago v. Mosley, 408 U.S. 92, 94-95 (1971) is inapposite. That case concerned an ordinance that allowed peaceful picketing only if it concerned one particular subject (a school's labor-management dispute), but not peaceful picketing on other subjects.

purpose of export controls on such software, and here the government's purpose is to limit the dissemination of products that can hinder U.S. intelligence collections efforts, and thereby harm foreign policy national security interests. Crowell Decl. ¶ 4; Lowell Decl. ¶ 4.[20] This is simply not a restriction on the content of ideas.[21]

Plaintiff's third theory as to why the ITAR is content-based largely echoes his second. He asserts that by "prohibiting" encryption software, the ITAR scheme "indirectly restricts a particular mode of speech." Pl. Mem. at 23. In other words, because encryption software scrambles and conceals communications on a computer, controls on its export are necessarily content-based. Plaintiff makes a related argument that export controls on encryption software "chills speech" by restricting the right of people to "speak confidentially." Pl. Mem. at 14.

What is primarily at issue with this contention is the right of foreign persons to use software exported from the United States to encrypt communications overseas. Plaintiff cites no authority for the proposition that the guarantees of the First Amendment extend to protecting the ability of foreign persons to use encryption in foreign lands, or that American citizens can provide them the means to do so. Indeed, a case on which plaintiff relies, United States v. United States District Court, 407 U.S. 297, 308 (1971), concerned the government's authority to undertake domestic wiretap surveillance without a search warrant, but expressly did not concern "the scope of the President's surveillance power with respect to the activities of foreign powers within or without this country." In any event, the ITAR regulates the

---

[20] See Karn v. Department of State, 925 F.Supp. 1, 10 (D.D.C. 1996) (appeal pending) (export controls on cryptographic source code are content-neutral and subject to intermediate scrutiny).

[21] Plaintiff's reliance on City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 429 (1993) again is off-point. There, the city barred only those newsracks from city streets which contained commercial information, but not for newspapers -- thus distinguishing between information able to be displayed based on its content. An evaluation of whether cryptographic software is subject to export based on whether it can be used to maintain the secrecy of information on a computer is hardly comparable to excluding publications from newsstands.

export of cryptographic software, not its usage in the United States or abroad.[22]

The Court of Appeals recent decision in Yniguez v. Arizonans for Official English, 69 F.3d 920 (9th Cir. 1995), cert. granted, 64 U.S.L.W. 3639 (March 25, 1996), does not resolve the standard of review issue in this case. There, the court held that Article XXVIII of the Arizona Constitution, requiring the use of the English language for all government functions, was not subject to review as a control on "expressive conduct" under United States v. O'Brien, 391 U.S. 367 (1968). In Yniguez, the court found that Article XXVIII required all Arizona state employees to use English in dealing with the public and that, as a result, "Arizonans who do not speak English will be unable to receive much essential information concerning their daily needs and lives." 69 F.3d at 936.

Plaintiff cites Yniguez for the proposition that "communications in language other than English" are a protectible "mode of expression" under the First Amendment. Pl. Mem. at 24. But export controls on cryptographic software are surely not analogous to an absolute bar on government employees from communicating other than through English. In Yniguez, governmental employees had no ability to express the content of any ideas, information, or thoughts to non-English speaking citizens. The "language" at issue here -- cryptographic source code -- is materially different since, whatever its communicative value, source code has a technical function: it can be programmed to encrypt information on a computer. While such "programming language" may be understood by those skilled enough to read it, its functionality implicates much more than merely speaking in English or Spanish. Hence, this case involves more than mere expression in "another language," but transmitting abroad a

---

[22] If export controls incidentally restrict the use of encryption software to protect conversations between individuals in the United States and foreign persons overseas, the same First Amendment analysis set forth herein would apply -- namely that such limitations are incidental to furthering a substantial governmental interest of protecting the government's foreign intelligence collection efforts.

product with technical capabilities.[23]

Moreover, while source code may be understandable to those knowledgeable enough to read it, the actual product of a cryptographic function is ciphertext -- scrambled letters and numbers that are not understandable to anyone. Ciphertext is certainly not a "language" of communication, but the result of a cryptographic process that cannot be understood unless one has the technical capability to decrypt the message. This underscores as well that the export of cryptographic software does not concern merely communicating in English, Spanish, or computer programming language, but providing the technical means to encrypt and decrypt information on a computer.

Plaintiff's mischaracterizes defendants' position, claiming we rely on O'Brien for the proposition that cryptographic software itself is "conduct." Pl. Mem. at 25. O'Brien is one of many cases that applied a lesser standard of review than strict scrutiny, in that case because the "speech" at issue was imbued with elements of conduct (burning a draft card). But the intermediate standard of review applies whenever the regulation of speech is content-neutral. See Turner, supra, (regulation of cable television); CCNV, supra, (prohibiting sleeping in park to demonstrate plight of the homeless). The intermediate standard of review is applicable here, not on the theory that "software" is "conduct," but because export controls on cryptographic software are content-neutral with respect to whatever communicative value such software has. See Def. Mem. at 23.[24]

---

[23] See Karn, 925 F. Supp. at 9 (rejecting analogy of source code to "foreign language" and the applicability of Yniguez since the ITAR does not regulate speaking in code). Other authority concerning the right to anonymous speech on which plaintiff relies is not apposite to the factual context here of exporting a cryptographic product. McIntyre v. Ohio Elections Comm'n, 115 S.Ct. 1511, 1516 (1995) (right of an individual to distribute anonymous political handbills); NAACP v. Patterson, 357 U.S. 449, 462 (1958) (right of the NAACP to preserve the confidentiality of its membership lists).

[24] Similarly, plaintiff's reliance on Minneapolis Star & Tribune Co. v. Comm. of Revenue, 460 U.S. 575 (1983) for the argument that cryptographic software is a tool of speech, like paper and ink, is without merit. In that case, the Supreme Court invalidated a statute which singled out publications for disparate taxation, a situation not comparable here. See Karn, 925 F. Supp. at 9, n.18 (rejecting similar argument that source code

B. Export Controls on Cryptographic Software Satisfy Intermediate Scrutiny.

Defendants have previously set forth the application of the intermediate standard of review to export controls on cryptographic software, see Def. Mem. at 18-25, and, therefore, primarily respond herein to plaintiff's argument on this issue. On the first aspect of the standard of review, whether there is a substantial governmental interest, Turner, 114 S.Ct. at 2469, plaintiff argues the government has not demonstrated such an interest in regulating "general academic and scientific publication on the subject of cryptography." Pl. Mem. at 27. Clearly, defendants do not assert this to be the interest at stake in this case, nor the purpose of ITAR controls. Rather, focusing on the export of cryptographic software, the government has put forward a substantial interest in protecting intelligence gathering efforts abroad, an interest deserving of great deference. See Def. Mem. at 20-23.[25] There is no genuine issue of material fact on this issue.

Plaintiff next argues that the ITAR scheme is not narrowly tailored, Turner, 114 S.Ct. at 2469, on the ground that the government "has adopted the most restrictive approach of prohibiting publication and communication about an entire subject area: the science of cryptography." Pl. Mem. at 27. This presents no analysis at all. Plaintiff again assumes his own conclusion that all such speech is prohibited, a proposition easily shown to be wrong. The government's purpose is to regulate the destination and end-use of software that has national security implications, and this is a matter quite distinct from "prohibiting publication" on the science of cryptography. See Def. Mem. at 23-25.

This leaves only the issue of whether the regulation is "unrelated to the suppression of speech." Turner, 114 S.Ct. at 2469. Among the more significant aspects of plaintiff's

---

diskette was a tool of speech).

[25] Plaintiff's reference to a 1980 newsletter on the issue of technical data controls, Pl. Mem. at 26, is particularly unfounded. The State Department has indicated its adherence to Edler in the Federal Register, and has amended the ITAR several times since 1980 to address First Amendment concerns. See Def. Mem. at 10-14.

pleadings is how strongly they confirm the most material of facts in this case: that cryptographic source code functions to encrypt information on a computer system. Plaintiff thereby concedes that the type of item at issue here is not a merely vessel of information or ideas, but one that can easily function to encrypt information. All of this is in accord with the record set forth by NSA Deputy Director Crowell concerning encryption.

For example, Bruce Schneier describes the "aim of encryption . . . to turn an otherwise intelligible message into gibberish, so that a person who intercepts the message cannot read it." Schneier Decl. ¶ 2; see Crowell Decl. ¶ 4, n.2.[26] That is precisely the concern with respect to foreign intelligence collection. Mr. Schneier explains further that encryption is based on an algorithm, a mathematical formula that transfers plaintext into ciphertext. Schneier Decl. ¶ 4; see Crowell Decl. ¶ 13. He also explains that an encrypted message cannot be read other than by those with access to the same key. Schneier Decl. ¶ 10-11; see Crowell Decl. ¶ 8 & n.5. Mr. Schneier also explains the importance of computers to cryptography.

> Cryptography is well suited for computers. Today, almost all cryptography is done by computers and dedicated computer chips. The reason for this is simple: modern cryptographic algorithms are a combination of mathematical and logical operations on bits and groups of bits. This is exactly the kind of thing that computers are so well suited for.

Schneier Decl. ¶ 15; see Crowell Decl. ¶ 19 (describing use of cryptographic software to encrypt on a computer).[27] Of even more significance, plaintiff also concedes that the steps necessary for using source code to actually encrypt data on a computer are trivial. See Declaration of Michael Paul Johnson ¶ 19 ("If I compile source code by pressing a button, I have a working program.") See Crowell Decl. ¶ 13 (compiling source code into object code is a trivial task).

Thus, while plaintiff argues that source code programming language has

---

[26] See also Declaration of Matthew Bishop ¶ 6.

[27] See also Bishop Declaration ¶ 7 (computers can be used to carry scrambled messages).

communicative value for academics trained in such matters, Pl. Mem. at 11-12; see Ellison Decl. ¶ 13 (describing programming as the creation of literature), he also sets forth the technical functionality of this commodity. This tracks what plaintiff told the State Department in his first letter: that Snuffle can be used to encrypt interactive conversation with zero-delay. See Tab 3 to Lowell Declaration. Indeed, plaintiff specifically said that he foresaw the "practical use" of Snuffle "for the purpose of interactively exchanging encrypted text." Id. Plaintiff's effort now to recast his purpose as a merely the "publication" of "ideas" should therefore not be credited. Having himself demonstrated that his software has a practical use to encrypt communications, the conclusion that export controls are unrelated to suppressing speech readily follows. See Karn, 922 F.Supp. at 10.[28]

III. THE ITAR IS NOT UNCONSTITUTIONALLY VAGUE.

Plaintiff sets forth a number of arguments that the statutory and regulatory scheme are impermissibly vague, all of which lack merit.

A. The Arms Export Control Act Is Not Void-For-Vagueness.

Plaintiff first claims that the Arms Export Control Act itself is impermissibly vague because it establishes broad discretion for the defendants to regulate defense articles and defense services in furtherance of world peace and national security, 22 U.S.C. § 2278(a), pursuant to which plaintiff claims that defendants regulate "academic and scientific publication." Pl. Mem. at 32-33. This claim is off the mark. Courts have long acknowledged that the AECA authorizes the Executive branch to regulate the export of information related to munitions, in recognition of the fact that national security could be threatened in this manner, as well as through the export of actual defense articles. See United States v. Van Hee, 531 F.2d 352, 355-56 (6th Cir. 1976); Edler, 579 F.2d at 521;

---

[28] Moreover, the fact that plaintiff and like-minded academics may intend to export source code solely to communicate ideas to other academics world-wide is immaterial, since the result would still be the availability overseas of cryptographic software in an indiscriminate fashion to recipients whose objective may be not to learn, but to use such products to conceal sensitive communications.

U.S. v. Posey, 864 F.2d at 1496. See Def. Mem. at 36-37. Thus, by itself, the statute sets forth a permissible objective. Moreover, on its face, the AECA does not purport to regulate scientific or academic exchange. For this reason, plaintiff's vagueness attack against the statute fails.

B. The Challenged Provisions of the ITAR Are Not Impermissibly Vague.

Replying next on OLC's 1978 memo, plaintiff claims that the ITAR exceeds the statutory authority in § 38 of the AECA by regulating academic exchange and publication. This claim assumes that the ITAR has gone unchanged in the past 18 years. As noted, since that time, the ITAR has been amended multiple times, Edler upheld the technical data provisions, and the State Department stated it would follow that approach. See Def. Mem. at 12-14. For plaintiff to suggest now that defendants have "leapt into the statutory void by defining 'export' to reach protected speech such as a professor's classroom teaching foreign students" is without any foundation.

1. The Definition of Cryptographic Software Is Not Vague.

Plaintiff next challenges several specific provisions of the ITAR as vague. He claims that the definition of cryptographic software as "capable of maintaining secrecy," 22 C.F.R. § 121.1, XIII(b)(1), gives little notice to persons of common intelligence." Pl. Mem. at 34. Plaintiff's declarants seem to understand what this term means. See Schneier Decl. ¶ 2 (aim of encryption is to turn intelligible messages into gibberish). Indeed, two of plaintiff's declarants describe it as virtually a term-of-art. They identify the distinction in Category XIII(b) between data "confidentiality, the ability to keep data private," and "authentication, the ability to identify both the sender of a message and that the message did not change in transit." Bishop Decl. ¶ 3. See also Johnson Decl. ¶ 10, 13 (distinguishing between "authenticating data" and "encrypting messages"). This is among the basic distinctions drawn by Category XIII(b). Indeed, the description of cryptographic software as "maintaining data secrecy or confidentiality" would strike academics in this area, as well as non-academics of

ordinary intelligence, as quite understandable.[29]

Plaintiff also argues that the definition of software is vague because it includes algorithms. Pl. Mem. at 35. Again, plaintiff's own declarants explain why the definition would be drawn in this manner. As one declarant points out, "[t]here is no reasonable distinction between 'software' and 'algorithm.' Both are descriptions of how to do some mathematical tasks." Johnson Decl. ¶ 14. If computer code is added to the algorithm, source code can be developed. Id. ¶ 18; see Crowell ¶ 13. Thereafter, source code can easily be compiled by pressing a button to obtain a working program. Johnson ¶ 19; see Crowell Decl. ¶ 13. Thus, there are good reasons why the term "algorithm" is included in the definition of software, since it is the heart of a cryptographic software program. See Schneier Decl. ¶ 4. At the same time, however, the publication of algorithms for peer review evaluation is a common practice, Crowell Decl. ¶ 22; Schneier Decl. ¶ 14, and, thus, the definition of software has not been applied to extend to algorithms merely set forth in academic journals or textbooks. See, e.g., Tabs 1, 4, 5 to Crowell Declaration.[30]

2. The Definitions of Defense Articles, Defense Services, And Technical Data Are Not Vague.

Plaintiff next argues that the key definitions of "technical data," "defense article," and "defense services" are vague because they "refer to each other in circular fashion." Pl. Mem. at 6, 34. From this, he contends that cryptographic software is both a defense article and technical data. Id. He also contends that "technical data" is defined to include "much scientific and technical information, including information about cryptography," and "export" to "include all manner of communication and general publication." Id. at 34. Plaintiff's rendition of regulatory provisions of the ITAR has two major flaws. First, plaintiff largely ignores those provisions which are essential to deciding whether the ITAR is a system of

---

[29] Also, the suggestion that cryptographic software necessary to secure important financial transactions is controlled as a defense article, see Bishop Decl. ¶ 8, is not accurate. See 22 C.F.R. § 121.1, XIII(b)(1)(ii), (v).

[30] See also Tabs 7 and 8 to the Coppolino Declaration.

prior restraint, or impermissibly vague -- the multiple exceptions to information controlled as technical data. Second, the provisions he does describe are set forth inaccurately.

First, cryptographic software is clearly listed separately in Part 121 of the ITAR, the "Enumeration of Articles" that comprises the United States Munitions List. See 22 C.F.R. § 121.1, XIII(b)(1). There can be no question that such software is "on" or covered by the USML. Plaintiff argues, however, that the term "defense article" includes technical data, see 22 C.F.R. § 120.6, and that technical data includes software. See 22 C.F.R. § 120.10(a)(4). The flaw in this reading is clear: while the definition of technical data includes some software, 22 C.F.R. § 120.10(a)(4), cryptographic software listed in Category XIII(b) is expressly excluded from the technical data licensing provisions. See 22 C.F.R. § 121.8(f). The very definition of "software" which plaintiff cites provides that those who wish to export software should apply for a technical data license unless the software is specifically enumerated on the USML -- citing the specific example of Category XIII(b). The meaning of this provision is not ambiguous: cryptographic software is not subject to the technical licensing provisions.[31]

Moreover, contrary to plaintiff's suggestion, "technical data" is in fact defined separately in the ITAR, and in a manner that distinguishes it from actual commodities treated as defense articles. Technical data means information "which is required for the design[,] development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles." 22 C.F.R. § 120.10(a) (emphasis added). As defined, technical data is not the defense article itself, but specific types of information concerning the article. The ITAR regulates the export of actual commodities (defense articles), information related thereto (technical data), and the provision of training and assistance to foreign persons

---

[31] The reason for this distinction between cryptographic software and technical data is simple, but important. Cryptographic software is not merely technical information that explains "how" a commodity works, it is the commodity. Such software can be loaded onto a computer and ultimately used to encrypt information. See Crowell Decl. ¶ 19.

in connection therewith (defense services). While such controls may be cross-referenced in the regulations, there are distinct regulatory provisions for each including, of most pertinence, a separate definition of technical data with its various exceptions.

3. The Exemptions To The Definition Of Technical Data Are Not Vague.

Plaintiff challenges as vague the very exceptions that exclude a host of information from export controls. These exemptions are far from vague. Plaintiff claims first that the exception for "scientific, mathematical, and engineering principles commonly taught in schools, colleges and universities" is vague, based solely on the notion that one school might not teach what another does. Pl. Mem. at 35. This argument can be quickly passed over. The ITAR does not purport to require uniformity in what schools teach. The obvious purpose of the exception is to indicate that technical data does not include information exchanged in the common, everyday occurrence of a university lecture. The ITAR does not indicate that the government must pass judgment on what can or cannot be deemed a "common" academic principle, nor is it so applied. Lowell Decl. ¶ 23.

Plaintiff's attack on the "public domain" exemption is also meritless. That provision contains several specific exceptions as to what is controlled as technical that any ordinary person can understand -- information in bookstores, newsstands, or disclosed at conferences. Plaintiff sees a "Catch-22" "lurking" in the provision that, unless something is already published, it is subject to export controls. He would construe the definition to mean, in other words, that nothing can be published without the government's approval. Not only is this wrong as a factual matter, see Lowell Decl. ¶ 22, it is by far the most un-reasonable interpretation of the provision, one that people of ordinary intelligence are least likely to assume is the case.[32]

[32] Plaintiff's discussion of the public domain provision is also highly confusing. He claims that "software" should be treated as in the public domain because that exception refers to "information," not "technical data." Pl. Mem. at 35-36. The public domain provision is a clear and express exception to the definition of "technical data." 22 C.F.R. § 120.10(a)(4) (technical data does "not include . . .information in the public

The origin of plaintiff's "Catch-22" theory was apparently his phone conversation with Charles Ray, formerly of the Office of Defense Trade Controls.[33] See Bernstein Decl. ¶¶ 23-31. This exemplifies, perhaps more than anything, the deficient manner in which plaintiff has presented his claims. Assuming, arguendo, that the transcript plaintiff submits of his conversation with Mr. Ray is authentic, it greatly undermines plaintiff's claims.

First, the conversation did not address whether Dr. Bernstein could or could not publish or export either Snuffle or his related paper, but concerned hypothetical applications of the public domain exception that plaintiff posed to Mr. Ray. Declaration of Charles Ray ¶ 6. Mr. Ray repeatedly made clear that he was not offering legal interpretations, but merely trying to assist the plaintiff in better understanding the ITAR. Id. ¶ 8. Mr. Ray also said he was not providing any determinations on behalf of the State Department that applied to plaintiff, and the conversation had nothing to do with plaintiff's CJ requests at issue in this case. Id. ¶ 6.[34] Indeed, according to his own transcript, plaintiff agreed that the discussion

domain as defined by § 120.11") (emphasis added). Thus, "information" in the public domain is quite obviously an exclusion from technical data controls. Meanwhile, cryptographic software is expressly excluded from technical data licensing procedures. See 22 C.F.R. § 121.8(f).

[33] This transcript was initially disclosed by plaintiff in June 1995, and defendants requested, but were never provided, a copy of the tape recording of this conversation, which plaintiff apparently still has since he claims to have edited the transcript in the interim. The Federal Rules of Evidence require the use of the original record, unless lost or destroyed or not obtainable by judicial process. F.R.E. 1002, 1004. The transcript also constitutes hearsay. For these reasons, it is inadmissible evidence. Pursuant to the Court's direction, the parties will confer on factual issues and file a joint statement of facts not in dispute on September 11, 1996. At the completion of this conferral process, should evidentiary disputes remain, defendants will submit a separate list of evidentiary objections, including as to any additional exhibits or declarations plaintiff's submit with their opposition brief on August 30, 1996.

[34] It is well-established that the government cannot be bound by the representations of any employee who does not have actual authority to make a binding determination or decision. Federal Crop Ins. Corp. v. Merrill, 332 U.S. 380, 384 (1947). For this reason, the frequent references in several of plaintiff's declarations to telephone conversations with government employees is highly suspect evidence. Aside from being hearsay, evidence of phone conversations with an employee lacks weight and relevance,

was hypothetical, and that he would not take Mr. Ray's views as "gospel."[35] Id..

Despite all of this, Mr. Ray's ultimate advice was sound and supported by case law: if the motive behind the publication of technical data related to a munition was to knowingly circumvent the ITAR, then this would have to be considered in assessing whether a violation occurred. Id. ¶ 7; see Edler, 570 F.2d at 522; Posey, 864 F.2d at 1496-97 (conduct of exporting technical data, even if publicly available, can be controlled if plaintiff intends to assist a foreign entity in developing or maintaining an item on the USML). This episode illustrates well that the basis of plaintiff's claims are his own misunderstanding, misreading, and misstatement of both the ITAR and of what he was advised by the government.

4. The Definition of Export Is Not Vague.

Plaintiff next challenges as vague the definition of an "export" of technical data as including disclosures to foreign persons in the United States. As defendants have explained, this definition cannot be viewed in isolation, but in connection with the exemptions to what is -- and is not -- regulated as technical data. See Def. Mem. at 29-30. Indeed, defendants agree with plaintiff that no reasonable person would view the regulations as controlling purely domestic publication on cryptography, Pl. Mem. at 36, which is why this aspect of the vagueness claim fails.

a. Transmission Over The Internet Presents Export Concerns.

Plaintiff also raises the issue as to whether Internet distribution of cryptographic software would constitute an export. Pl. Mem. at 36-37. As a threshold matter, the question

---

since such conversations do not reflect the actual discharge of legal authority by responsible agency officials.

[35] Not only did he take them as "gospel," plaintiff avers in his Complaint that Mr. Ray told him "in essence that his Scientific Paper could never be placed in the public domain since it is not already in the public domain." Compl. ¶ 156. By plaintiff's own account, this greatly mischaracterizes the statements of Charles Ray. Plaintiff then sued Mr. Ray in his individual capacity.

of posting source code to the Internet was not addressed by the government administratively in resolving Dr. Bernstein's CJ requests. The sole governmental action in this case was a "commodity jurisdiction" determination. The government decided only that plaintiff's software was covered by Category XIII(b) of the USML and subject to the export licensing jurisdiction of the State Department. What this means is that, if the plaintiff sought to export his software, in whatever manner, he must first obtain a license from the State Department. Plaintiff did not do so, and no administrative determination was made as to whether (or how) he could export his software. Thus, while plaintiff has indicated that he wishes to export the Snuffle on the Internet, a CJ determination itself goes to the status of the commodity, and not its means of export or its intended destinations. The latter is for a licensing determination. Put another way, if the State Department had determined that Snuffle was not covered by the USML, this determination would be equally applicable to whatever means of export exists, not merely through the Internet.

That said, plaintiff's contention that distribution through the Internet would not implicate the notion of an export, Pl. Mem. at 36-37, is highly suspect. The Internet is an international telecommunications medium, through which information on "World-Wide Web" or FTP sites, or posted to "newsgroups" such as sci.crypt, can be accessible internationally. Plaintiff himself stated in his first CJ request that he wished to distribute Snuffle to the "worldwide" academic community through sci.crypt. Tab 3 to Lowell Declaration.[36]

As the State Department recently explained to plaintiff in connection with his upcoming teaching activities, the Internet is still a fairly recent phenomenon with implications for U.S. security interests that the State Department must consider. See Tab 24 to Lowell Declaration (July 25, 1996 Letter). There is the obvious concern that posting software

---

[36] Plaintiff fails to cite the most salient findings made concerning the Internet in the district courts opinion at the preliminary injunction stage in ACLU v. Reno, 1996 U.S.Dist. Lexis, 7919 (E.D. Pa. June 11, 1996) (Part II, Findings of Fact) (¶ 3 - an estimated 40% Internet host computers are overseas); (¶ 4 - the Internet is an international system); (¶ 25 - USENET newsgroup servers are located throughout the world); (¶ 33 - the World Wide Web provides international links between computers).

without regard to whether it can be distributed to international destinations would circumvent ITAR controls. Id. Hence, the State Department has advised parties, including plaintiff, to take reasonable steps to confine the distribution of software to Internet sites within the United States and Canada, based on technical means that appear to be available to do so. Id.[37] Given the international structure of the Internet, and its implications for so easily transmitting cryptographic software for immediate downloading and use, defendants' position is not unreasonable. Moreover, the issue of Internet distribution concerns the means of export, not whether controls on the actual item being exported violates the First Amendment.[38]

IV. ITAR EXPORT CONTROLS ON TECHNICAL DATA AND CRYPTOGRAPHIC SOFTWARE ARE NOT OVERBROAD.

A. Plaintiff Cannot Show That the ITAR Is Substantially Overbroad.

Plaintiff uses the overbreadth doctrine to again claim that the ITAR impermissibly regulates academic and scientific publication. See Compl. ¶¶ 152, 153, 157. He must therefore show that the ITAR is substantially overbroad in relation to the statute's plainly legitimate sweep, and incapable of a narrowing, constitutional construction. Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973); United States v. Stansell, 847 F.2d 609, 613 (9th Cir. 1988). See Def. Mem. at 28-29. Export controls on commodities and technical data do indeed have a plainly legitimate sweep, as courts have found. See Def. Mem. at 20.

---

[37] If such steps are taken, the posting of academic course materials for students on a Web site, Bernstein Decl. ¶ 61, may not present export concerns, even assuming the software to be posted is covered by the USML. Tab 24 to Lowell Declaration.

[38] Some of plaintiff's declarants describe the distribution of source code on the Internet as part of the process of exchanging of academic information. See, e.g., Declaration of Andrew W. Appel ¶ 14; Declaration of Richard Stallman ¶ 8; Declaration of Dr. Paul Ginsparg. First, this case concerns cryptographic source code, not all source code in general, which these declarants appear to describe. See, e.g., Ginsparg Declaration, Appendix A and B (containing non-cryptographic source code). Second, the ITAR does not regulate the domestic distribution of cryptographic software, including domestic exchanges of source code among academics. Third, as the court held in Karn, the fact that some cryptographic source code may be available on the Internet is a policy matter that does not justify the elimination of export controls on such software. Karn, 922 F. Supp. at 11.

The question, then, is whether the ITAR is so overbroad with respect to cryptographic technical data and software that it must be struck down in all applications as to such items. Plaintiff relies (again) on the 1984 OLC analysis that the ITAR's technical data provisions could arguably encompass a technical lecturer at a university or theoretical discussion with foreign persons. Pl. Mem. at 38. But far more so than when Edler was decided in 1978, or when OLC last opined in 1984, current ITAR technical data controls make express exemption for information exchanged through teaching, publication, and fundamental research. As such, the regulations are even more susceptible to a construction that, on their face, the government does not seek to regulate the academic exchange of information -- particularly since the government itself construes and applies the provisions this way.[39]

B. Other Administrative Cases Plaintiff Cites Do Not Support His Overbreadth Claim That The ITAR Reaches Academic Freedom.

Plaintiff presents a number of cases involving third parties who, like plaintiff, sought to export cryptographic software products.[40] A review of these submissions indicates not only a lack of overbreadth reaching academic freedom, but a consistent focus by the government on the export of actual cryptographic software.[41]

---

[39] Controls on cryptographic software do not present overbreadth concerns since they do not apply to all cryptographic functions, but to software that can maintain data confidentiality. 22 C.F.R. § 121.1, XIII(b). As such, controls are focused on a commodities that could most directly have a harmful impact on national security and foreign policy interests since they could be used to hinder foreign intelligence collection efforts. None of the OLC opinions concluded that export controls on actual commodities, such as cryptographic devices and software, implicate First Amendment concerns. The sole issue OLC analyzed was the reach of the technical data controls.

[40] This, apparently, is the showing plaintiff has previously represented he would make "that the speech of other individuals known to him has been restrained in that they have restrained from publishing for fear of violating the AECA." Declaration of Cindy A. Cohn ¶ 5 (submitted pursuant to Fed.R.Civ.P. 56(f)) (September 21, 1995).

[41] As defendants have previously noted, since an "overbreadth" claim seeks to invalidate the statute as to all conceivable applications, including those of parties not present, courts look to whether the plaintiff seeks to vindicate interests that are dissimilar to his own. Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 503 (1984); Def. Mem. at

For example, Bruce Schneier refers to the export status of diskettes containing source code described in his book, *Applied Cryptography*. Schneier Decl. ¶ 27. This very issue was litigated in the Karn case and the government has thus far prevailed. The diskette at issue in Karn contained source codes that could readily be compiled and executed to encrypt. The court found the government's interest in controlling this export to be substantial, and held that such action did not violate the First Amendment. Karn, 925 F. Supp. at 11-12.

Other declarants purport to describe their own dealings with the government concerning cryptographic software. But theses cases, likewise, concern the export of software, including for commercial reasons, and therefore, present no genuine issue of material fact as to plaintiff's overbreadth claim that technical lectures or the mere publication of scientific ideas are regulated by the ITAR.

Michael Paul Johnson indicates that, despite his frustration with the process, he received a favorable CJ determination that his "Quicrypt" commercial software product was subject to the export licensing jurisdiction of the Commerce Department. Johnson Decl. ¶ 31.[42] According to Mr. Johnson, at issue was the length of the "key" of his product -- a

---

25-27. See, e.g., Yniguez, 69 F.3d at 932 (plaintiff seeks to vindicate not only her own interests, but those of all government employees in different jobs, as well as those of non-English speaking citizens). Here, plaintiff's overbreadth claim, raised on his own behalf and those of third parties, raises the same issue as to whether the ITAR restricts the academic publication of ideas, including through export controls on cryptographic software. Since there is no want of a proper party before the court on this issue, invalidation of the ITAR on its face as to all other applications (for example, to commercial products) should not be considered. See Lind v. Grimmer, 30 F.3d 1115, 1123 (9th Cir. 1994) (when a statute's only unconstitutional application is the one directed at a party before the court, there is no justification for declaring the statute invalid in all its applications), cert. denied, 115 S.Ct. 902 (1995).

[42] The Johnson Declaration contains hearsay accounts of statements purportedly made by government employees on the phone. See, e.g., Johnson Decl. ¶ 27. Even if his rendition of these conversations were admissible, see n.34 supra, Mr. Johnson indicates that NSA informed him that he could "freely use and distribute [his] program in the United States." Id. ¶ 24. Mr. Johnson also indicates that the government requested a complete rendition of the software for evaluation before advising him on its exportability, id., -- a reasonable and understandable position.

matter which goes to the effectiveness of the software. See Crowell Decl. ¶ 8 n.5 (in general, the longer the key space, the greater the complexity and significance of the software for encrypting data). Assuming, arguendo, the truth of his averments, the government's actions are consistent with its position herein: Mr. Johnson's commercial cryptographic software product was evaluated for its capability.[43] None of this implicates First Amendment interests in "academic freedom" that Dr. Bernstein seeks to vindicate through his overbreadth claim.

Similarly, Brian Behlendorf alleges that the government had concern with aspects of certain Internet "Web-server" software. Mr. Behlendorf says he was told by another software developer that NSA had determined that the software would violate the ITAR due to "hooks" in the program that allow users to add separately-available encryption software programs. Behlendorf Decl. ¶ 5. Assuming arguendo this is correct,[44] it is not material to Dr. Bernstein's overbreadth claim, which alleges that export controls on technical data encompass mere academic expression. Rather, the dispute described by Mr. Behlendorf concerns how a particular software product can be made capable of functioning to encrypt. As Mr. Behlendorf explains, "Hooks are part of a computer program that allow one to add new code to the original software easily," id. ¶ 5, in this case software with encryption capabilities. Indeed, the software "hooks" were specifically designed for encryption software, and the program was intended for world-wide distribution. Behlendorf Decl. ¶ 5, 7-8. This presented obvious export control issues. In any event, this dispute does not involve overbreadth concerns that the ITAR limits "academic freedom."

Next, plaintiff discusses the case of James T. Demberger and the posting of

---

[43] See also Tab 20 to Lowell Declaration describing technical specifications, including key length, for mass-market products subject to transfer to the Commerce Department's jurisdiction.

[44] This statement is hearsay.

cryptographic source code to the Internet. The gravamen of this dispute is whether cryptographic software should have been treated as technical data and subject to the public domain exception. See Demberger Declaration. As has been explained herein, the government treats cryptographic software as a defense article, and not technical data, because such software is not mere "know how" explaining how cryptography works, but an actual commodity that can be made to encrypt communications on a computer. Crowell Decl. ¶ 19. As with plaintiff, Mr. Demberger apparently disagrees with this reading and application of the regulations. The matter at issue, however, is not "academic freedom," or the "publication of scientific ideas," but whether software that can easily be used to encrypt should be indiscriminately transmitted world-wide.

Lastly, plaintiff cites two other cases, involving a law professor and a student, which again do not indicate that the government impermissibly applies the ITAR. The law professor is Peter D. Junger, who claims, inter alia, that he is required by the ITAR to expel foreign students from his class on cryptography and the law. See Junger Decl. ¶ 25. As such, he has the same misconceptions as plaintiff as to the reach of the ITAR, and presents no additional overbreadth aspect of the issue.[45]

Prof. Junger also apparently wishes to export cryptographic software through the Internet. The fundamental flaw with the Junger case, however, is the lack of any meaningful administrative proceedings at all. Prof. Junger did not submit his software for an assessment by the State Department or NSA as to whether it was subject to export controls under the USML. The government was left to figure this out on its own. Assuming his software is covered by the USML, controls on its export would not violate the First Amendment, for the

[45] The Junger Declaration also contains hearsay descriptions of what purport to be phone contacts with government employees. Junger Decl. ¶¶ 9-15. Even if this were admissible, Prof. Junger states he was advised that teaching about his software would not cause a problem, but posting it to the Internet was a "gray area." Id. ¶ 11.

reasons set forth herein.[46]

Plaintiff also submits a declaration from Lawrence Miller, who alleges that as a student at George Washington University, he had to take an "incomplete" in a class on Computer Security Systems because of ITAR controls. Specifically, he claims that he could not fulfill a course requirement to placed a project on an Internet's World Wide Web site that included "a cryptographic key management and certification system." Miller Decl. ¶ 7. On November 16, 1995, less than a month before his project was due, Mr. Miller and his professor, Lance Hoffman, wrote a letter to the State Department describing the matter.

The State Department responded on December 15, 1995, pointing out that the ITAR does not extend to regulate scientific or mathematical or engineering principles commonly taught in colleges and universities, and that "[n]o license is required for the activities described in your letter so long as no cryptographic software covered under Category XIII(b) of the United States Munitions List is taken or sent outside the United States." Exhibit D to Miller Declaration (emphasis added). The Department did not indicate that the mere exchange of ideas concerning cryptography in an academic setting was regulated.

Mr. Miller apparently had several questions concerning this response, but states that he did not follow-up with the State Department. Miller Decl. ¶ 38, 39. As with Prof. Junger, Mr. Miller did not submit the actual software at issue in his project for a commodity jurisdiction determination. Despite this, Mr. Miller seems to ascribe blame to the State Department for his incomplete grade. The State Department cannot answer questions it is not asked, and the fact that Mr. Miller received an incomplete grade was a determination made by his professor. The Department tried to answer the questions it was presented with, indicated that the activities Mr. Miller described were not covered, and did not seek to

---

[46] Prof. Junger recently filed his own lawsuit and motion for a preliminary injunction on August 8, 1996. Defendants moved to dismiss for lack of ripeness and standing, and for summary judgment, on August 22, 1996. To set forth the background of this case further, a copy of the Declarations of William J. Lowell and William P. Crowell filed in Junger v. Christopher, Case No. 96 CV 1723 (N.D. Ohio) are submitted herewith at Tabs 4 and 5 to the Coppolino Declaration.

interfere in this matter.[47]

C. Plaintiff's Attempt to Distinguish Edler Is Without Merit.

In his discussion of overbreadth, plaintiff attempts to distinguish Edler Industries, the case which undercuts all of his claims concerning technical data. He argues first that Edler concerned only technical data, not defense articles. Pl. Mem. at 40. This is correct, but defendants have relied on Edler precisely to show that current technical data controls are not overbroad. Moreover, Edler does support a finding that controls on defense articles, including cryptographic software, are constitutional as well. If the conduct of providing technical assistance in connection with a defense article can be controlled, 579 F.2d at 521, surely controls intended to restrict access to a commodity that can function to encrypt communications are a permissible effort to control the flow of items that have national security and foreign policy applications. Id. at 520. Plaintiff also notes that the current ITAR definitions were amended since Edler was decided. Pl. Mem. at 40. Indeed, they were amended several times, -- expressly for the purpose of making clearer that speech activities are not subject to regulation. See Def. Mem. at 12-14.

Plaintiff also claims that by defining software as a defense article, and not as technical data, defendants seek to "escape" the narrowing construction in Edler by mere "labels." Pl. Mem. at 40. He avers that this "mocks the Ninth Circuit" because plaintiff must obtain a license to "publish Snuffle as part of the scientific exchange of ideas and information extolled in Edler." Id. at 41. It is plaintiff's characterization that mocks the facts.

First, this is not a matter of mere labels. Cryptographic software is properly treated as a defense article because it is not mere "know how" about cryptography. Crowell Decl. ¶ 19. Plaintiff and his declarants explain well that his software, and that like it, does much

---

[47] Mr. Miller states that, nearly two months later, Professor Hoffman sent a private email to the home of an employee of the Office of Defense Trade Controls, who happened to be a student himself of Prof. Hoffman at GWU. Miller Decl. ¶ 41. Particularly given the close proximity between the George Washington University and the State Department in Washington, Mr. Miller or Prof. Hoffman could easily have sought clarification through more formal channels of authority.

more than inform, but has a practical use -- in the case of Snuffle to provide for zero-delay encrypted conversations. Moreover, what plaintiff seeks to do is not merely "publish ideas" but export, without limitation to anywhere in the world, a commodity that he and his declarants have explained has a practical cryptographic function. To describe this merely as "publishing" an "idea" is disingenuous. The government's action is fully consistent with how Edler and several other courts, see Def. Mem. at 20, have upheld the application of export controls to matters that have national security and foreign policy significance.

CONCLUSION

For the foregoing reasons, defendants' motion for summary judgment should be granted, plaintiff's motion for summary judgment should be denied, and this action should be dismissed with prejudice.

Respectfully Submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

MARY BETH UITTI
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198

by MB Uitti
Anthony J. Coppolino

VINCENT M. GARVEY
ANTHONY J. COPPOLINO
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470 or 616-8460

Attorneys for the Defendants

CERTIFICATE OF SERVICE

I hereby certify that on this the 30th day of August 1996, a copy of the foregoing memorandum of points and authorities in opposition to plaintiff's motion for summary judgment and in further support of defendants' motion for summary judgment was served, via overnight express mail, on:

Cindy A. Cohn
McGLASHAN & SARRAIL
177 Bovet Road, Sixth Floor
San Mateo, California 94402

and

Lee Tien
1452 Curtis Street
Berkeley, California 94702
(510) 525-0817

by HB Authority
Anthony J. Coppolino
ANTHONY J. COPPOLINO

EXHIBIT T

International Traffic in Arms: Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

Docket Folder Summary View all documents and comments in this Docket

Docket ID: DOS-2015-0023 **Agency:** U.S. Department of State (DOS)

RIN: 1400-AD70 **Impacts and Effects:** International **CFR Citation:** None
Priority: Other Significant

+ View More UA and Regulatory Plan Information and Docket Details

Take a Tour!

Sign up for Email Alerts

9,985
Comments Received*

Tweet Share Email

Primary Documents View All (1)

PR International Traffic in Arms: Definitions of Defense Services, Technical Data, and Public Domain...
Proposed Rule **Posted:** 06/03/2015 **ID:** DOS-2015-0023-0001
Comment Period Closed
Aug 03, 2015 11:59 PM ET

Supporting Documents

No documents available.

Comments View All (9,985)

To whom it may concern: I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State..."
View Comment **Submitter Name:** Anonymous Anonymous **Posted:** 08/04/2015
ID: DOS-2015-0023-9115

To whom it may concern: I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State..."
View Comment **Submitter Name:** Wesley Gilden **Posted:** 08/04/2015 **ID:** DOS-2015-0023-9112

To whom it may concern: I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State..."
View Comment **Submitter Name:** Mike Taylor **Posted:** 08/04/2015 **ID:** DOS-2015-0023-9111

this bill is dumb once again u missed the point. what happened to the freedom of information act????????????"
View Comment **Submitter Name:** don catena **Posted:** 08/04/2015 **ID:** DOS-2015-0023-9110

To whom it may concern: I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State..."
View Comment **Submitter Name:** Ed Gillett **Posted:** 08/04/2015 **ID:** DOS-2015-0023-9109

Regulatory Timeline

Pre Rule
Proposed Rule
Final Rule
Completed
Current Stage

Agency Contact

C Edward Peartree
Director, Office of Defense Trade Controls Policy
DOS
ddtcresponseteam@state.gov
202 663-2792
2401 E Street NW., ATTN: ITAR Amendment
Washington, DC 20522

*This count refers to the total comment/submissions received on this *docket*, as of 11:59 PM yesterday. Note: Agencies review all submissions, however some agencies may choose to redact, or withhold, certain submissions (or portions thereof) such as those containing private or proprietary information, inappropriate language, or duplicate/near duplicate examples of a mass-mail campaign. This can result in discrepancies between this count and those displayed when conducting searches on the Public Submission document type. For specific information about an agency's public submission policy, refer to its website or the Federal Register document.